
Electronic Theses and Dissertations

2019

An Algorithm for inferring consumer-to-consumer trust on twitter

Dennis Loyatum
Faculty of Information Technology (FIT)
Strathmore University

Follow this and additional works at <https://su-plus.strathmore.edu/handle/11071/6706>

Recommended Citation

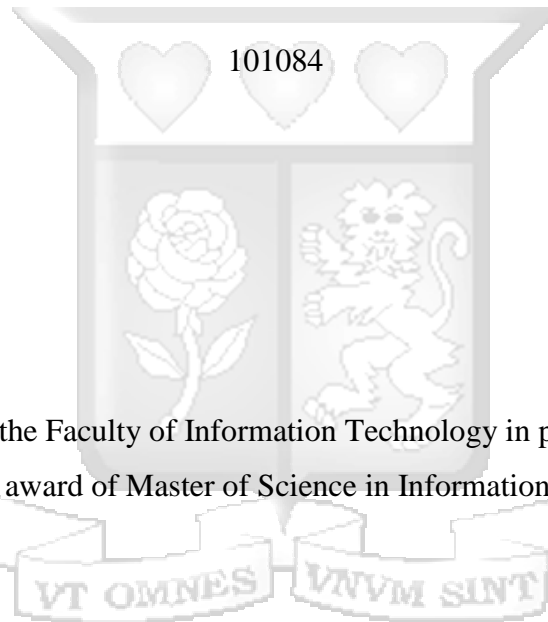
Loyatum, D. (2019). *An Algorithm for inferring consumer-to-consumer trust on twitter* (Thesis, Strathmore University). Retrieved from <http://su-plus.strathmore.edu/handle/11071/6706>

This Thesis - Open Access is brought to you for free and open access by DSpace @Strathmore University. It has been accepted for inclusion in Electronic Theses and Dissertations by an authorized administrator of DSpace @Strathmore University. For more information, please contact librarian@strathmore.edu

An Algorithm for Inferring Consumer-to-Consumer Trust on Twitter

By

Dennis Loyatum



A Thesis Submitted to the Faculty of Information Technology in partial fulfillment of the requirements for the award of Master of Science in Information Technology degree.

Faculty of Information Technology

Strathmore University

Nairobi, Kenya

June 2019

Declaration and Approval

I declare that this work has not been previously submitted and approved for the award of a degree by this or any other University. To the best of my knowledge and belief, this research thesis contains no material previously published or written by another person except where due reference is made in the thesis itself.

© No part of this thesis may be reproduced without the permission of the author and Strathmore University

Name of Candidate: Dennis Kibet Loyatum

Signature:

Date:

Approval

The thesis of Dennis Kibet Loyatum was reviewed and approved by the following:

Dr. Bernard Shibwabo

Signature:.....

Date:.....

Senior Lecturer & Director, Research and Postgraduate Studies

Strathmore University

Abstract

Trust amongst users engaged in consumer-to-consumer (C2C) e-commerce on Twitter as well as other social media platforms has been on the decline. The cost effective manner and timely delivery of C2C content makes it possible to reach a wider consumer base across the globe. However, this is under threat partly because of the risk of being scammed by other consumers on these platforms and the uncertainty related to this kind of e-commerce. Social media platforms such as Twitter are experiencing a decline in active user partly because of misuse of their platform.

Twitter features can be used to build a consumer-to-consumer trust inference algorithm that can be relied upon by consumers in determining who to engage with in C2C e-commerce for specific contexts having not interacted directly with the seller/buyer in the physical world. There is a need by consumers to know whom they can trust on important C2C e-commerce transactions to limit their exposure to scams and fraudulent users on Twitter.

This research sought to develop an algorithm to infer the trust score of a user engaged in consumer-to-consumer e-commerce using features present on his/her user profile. The algorithm utilized machine learning techniques. The algorithm provides consumers with a sense of trust in C2C engagements on Twitter. The research employed an experimental approach that involved the development of an algorithm and its validation. Wrapper approach was adopted for feature selection using data mined using Twitter Search API using C2C keyword-hashtag (#). Multi-class classification was successfully applied to infer a consumers trust score. Potential users can then use the proposed algorithm to check and choose trusted consumers on Twitter for different transactions.

Keywords: Social media, Consumer-to-consumer trust, E-commerce, Feature Selection, Machine Learning Algorithm

Table of Contents

Declaration and Approval	ii
Abstract	iii
List of Figures	ix
List of Tables	x
List of Abbreviations	xi
Chapter 1: Introduction	1
1.1 Background to the study	1
1.2 Problem Statement	2
1.3 Aim	3
1.4 Specific Objectives	3
1.5 Research Questions	3
1.6 Justification	3
1.7 Scope and Limitation	4
Chapter 2: Literature Review	5
2.1 Introduction	5
2.2 E-Commerce Business Models	5
2.3 Consumer-to-Consumer (C2C) e-commerce	6
2.4 Concept of Trust in Social Media	7
2.5 Dimensions Determining Trust	8
2.6 Trust Metrics in Social Networks	9
2.7 Properties of Trust	10
2.8 Trust Contexts	11
2.9 Existing Approaches of Trust Computation	12
2.10 Trust Computation on Social Media	13
2.11 Machine Learning Approach to C2C Trust on Twitter	13
2.11.1 General Trust Prediction Model	13
2.11.2 Feature Selection	14
2.11.3 Filter Approach	15
2.11.4 Wrapper Approach	16
2.11.5 Hybrid Approach	17

2.12	Machine Learning (ML) Algorithms	17
2.12.1	Decision Tree	18
2.12.2	Random Forest	19
2.12.3	Support Vector Machines	19
2.12.4	Naïve Bayes	19
2.12.5	K-Nearest-Neighbor (KNN)	20
2.13	Conceptual Framework	20
Chapter 3:	Research Methodology	22
3.1	Introduction	22
3.2	Research Design	22
3.3	Population and Sample	22
3.4	Data Collection Instrument	23
3.4.1	Mining Twitter	23
3.5	Data Preprocessing	25
3.6	Model Training	25
3.6.1	Feature Weighting	26
3.7	System Development Methodology	27
3.7.1	Overview of RAD Structure	27
3.7.2	Phases of RAD	27
3.7.2.1	Requirements Planning Phase	27
3.7.2.2	Design Phase	28
3.7.2.3	Construction Phase	28
3.7.2.4	Transition Phase	28
3.8	Validity and Reliability	28
3.9	Ethical Consideration	29
3.10	Research Evaluation	29
3.10.1	Accuracy	30
3.10.2	Precision	30
3.10.3	Recall	31
3.10.4	F-Measure	31
3.11	Model Validation	31
Chapter 4:	Analysis and Design	32
4.1	Introduction	32

4.2	Requirement Analysis	32
4.2.1	Functional Requirements	32
4.2.2	Non-Functional Requirements	32
4.2.3	Usability	32
4.2.4	Scalability	33
4.2.5	Storage	33
4.3	Proposed Algorithm	33
4.4	System Architecture	35
4.5	Diagrammatic Representation of the Algorithm	36
4.5.1	Use Case Diagram	36
4.5.2	Detailed Use Case Descriptions	37
4.5.3	Sequence Diagram	39
4.5.4	Context Diagram	40
4.5.5	Data Flow Diagram	41
Chapter 5:	Algorithm Implementation and Validation	42
5.1	Introduction	42
5.2	Building the Dataset	42
5.3	Training the Model	43
5.4	Testing the Model	44
5.5	Using the Model for Feature Selection	45
5.6	Validation	46
5.7	Trust Score Assignment with All Features	46
5.8	Trust Score with Selected Features	47
Chapter 6:	Discussions	48
6.1	Introduction	48
6.2	Discussions	48
6.3	Limitations of the Proposed Algorithm	49
Chapter 7:	Conclusion and Recommendations	50
7.1	Conclusion	50
7.2	Recommendations	51
7.3	Future Work	51
References	52

Appendix A: Originality Report	56
--------------------------------------	----



List of Equations

Equation 3.1	26
Equation 3.2	30
Equation 3.3	30
Equation 3.4	31
Equation 4.1	33
Equation 4.2	33
Equation 4.3	33
Equation 4.4	34



List of Figures

Figure 2.1 : C2C E-commerce Business Model	7
Figure 2.2 : Pipeline of Trust Prediction Models	14
Figure 2.3 : Filter-Based Feature Selection	16
Figure 2.4 : Wrapper Feature Selection	16
Figure 2.5 : Conceptual Framework	21
Figure 3.1 : Importing Twitter Search Data.....	25
Figure 3.2 : RAD Life Cycle Stages	27
Figure 3.3: Sklearn Feature Selection Code Snippet	28
Figure 4.1 : System Architecture	36
Figure 4.2 : Proposed Algorithm Use Case	37
Figure 4.3 : Search Tweets Use Case.....	38
Figure 4.4 : Assign Trust Score Use Case	39
Figure 4.5 : Sequence Diagram.....	40
Figure 4.6: Context Diagram	40
Figure 4.7 : Level 0 DFD.....	41
Figure 5.1: Dataset Description	43
Figure 5.2 : Loading Data to Pandas DataFrame.....	43
Figure 5.3 : Numpy-array Representation of Training Data.....	43
Figure 5.4 : Feature Selection with Logistic Regression Module.....	45
Figure 5.5 : Feature Selection using Logistic Regression.....	46
Figure 5.6 : Feature Comparison	47

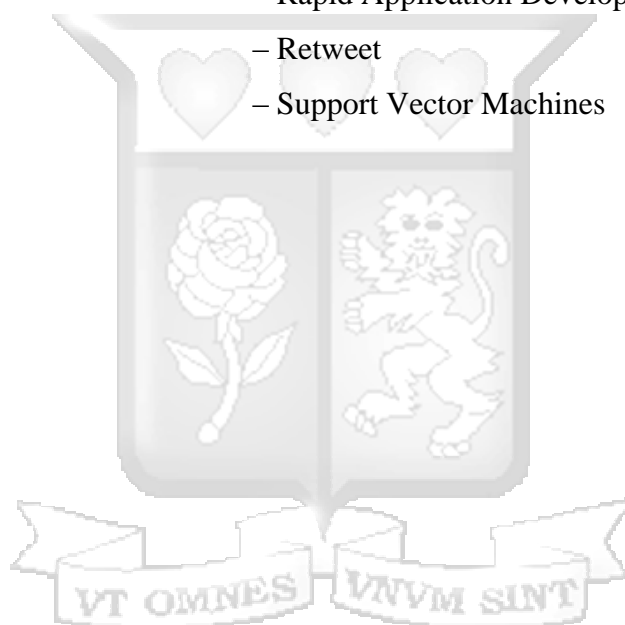
List of Tables

Table 2:1: Comparison of Typical Classifiers	18
Table 3:1 Sample of Selected Features	24
Table 3:2 : Confusion Matrix.....	29
Table 4:1: Description of Selected Features Based on Profile	34
Table 4:2: Pseudocode of the Proposed Algorithm	35
Table 5:1 : Confusion Matrix for KNN	44
Table 5:2 : Confusion Matrix for RF	44



List of Abbreviations

API	– Application Programming Interface
B2B	– Business-to-Business
B2C	– Business-to-Consumer
C2A	– Consumer-to-Administration
C2C	– Consumer-to-Consumer
DAU	– Daily Active Users
KNN	– K-Nearest Neighbor
MAU	– Monthly Active Users
NB	– Naïve Bayes
RAD	– Rapid Application Development
RT	– Retweet
SVM	– Support Vector Machines



Chapter 1: Introduction

1.1 Background to the study

The Internet in this era has currently penetrated to almost all corners of the world. Technology is affecting the way we communicate and do business. For example, selling products has evolved from brick and mortar stores to e-commerce websites, and now to social media. Consumers have adopted social media to conduct e-commerce because of the various benefits that it presents, a concept termed social commerce (Stephen & Toubia, 2009). The reduction in the cost of these products and services is due to elimination of middlemen, ability to reach a wide audience and significant increase in the use of smartphones (Transparency Market Research, 2017). Social media is improving local and international commerce (Kumah, 2014).

Shopping through social media may well be a key channel of the future such as C2C commerce (Richard & Guppy, 2014; Chahal, 2016). Social media has become an important medium for retail sales and consumer-to-consumer interactions; in this regard, social media has become an important tool for consumers (Richard & Guppy, 2014). Consumer trust on Twitter is on the decline (Arnold, 2019). According to Forbes (2019), globally, only 41% of people indicate they trust social media platforms.

In the USA, e-commerce sales grew by 16% in 2017 (Digital Commerce 360, 2018). Globally, the number of Internet users stood at 3.4 billion in 2016 and 39.4 million users in Kenya (Communications Authority of Kenya, 2018). If the trust of consumer-to-consumer e-commerce is increased in social media, consumers will be more willing to engage in consumers-to-consumer business. Van der Heijden et al. (2003) identified two types of issues that affect consumers' online purchases decisions, which were technology and trust.

The overall effect of social networks on the consumer has been to increase the power that consumers over other consumers and businesses (Malthouse et al., 2013). Like B2C e-commerce, building consumer trust in C2C e-commerce can be a challenge (Gustavsson & Johansson, 2006). Gustavsson and Johansson (2006) urged that physical clues are absent in the online environment, the researcher holds the opinion these clues are present in social media but need to be identified and used to develop an algorithm for inferring consumer-to-consumer trust on Twitter.

1.2 Problem Statement

The wide adoption of social media as a platform of C2C e-commerce necessitates that users trust each other in order to transact but this has not been the case. The Daily Active Users (DAU) to Monthly Active Users (MAU) Ratio measures the stickiness of social media platforms. That is, how often people engage in social media platforms, this ratio is ever on the increase but is under threat because of low trust levels (Statistica, 2019).

The lack of trust on social media presents a problem to both users and social media providers. For users, there is an uncertainty risk among consumers intending to engage in consumer-to-consumer e-commerce on social media. This source of risk is uncertainty regarding the intention of the other party or user (Gustavsson & Johansson, 2006). Both parties are interdependent on each other and therefore there is a need to determine the trust level amongst these potentially mutually beneficial parties. Social media platforms are be rife with consumer-to-consumer scams; users can pay for products/services and have them delivered late, sub-standard or never at all (Bao & Volkovynska, 2016; Communications Authority of Kenya, 2018; Dan, 2014).

The loss of trust by users presents a problem to social media providers, as consumers will stay away from these platforms. Participation in consumer-to-consumer e-commerce on Twitter requires a user trusting both the social media platform, on which C2C is performed, and the other user involved in a transaction (Bao & Volkovynska, 2016). Another problem presented to social media platforms is employing more people to review reported abuse content and users (Dignan, 2019). There are renewed efforts by Twitter to employ Artificial Intelligence (AI) algorithms to enforce community standards (Twitter, 2019).

The present survey-based recommendation/reviews approach to measuring trust amongst consumers is rigid and does not take into count dynamics of user activity on social media specifically Twitter. Today's approach to trust in Twitter is often binary—either you are banned or not after defrauding another consumer (Dignan, 2019). Consumers will unconsciously build a level of trust based on their social media networks activity such as likes, retweets, posts, and comments among others (Richard & Guppy, 2014). Twitter features used to compute trust vary from user to user and from context to context. Also, trust features of a certain context might change along the way in order to incorporate more useful trust features for a particular context (Lopez & Maag, 2015).

There is therefore need to develop a novel approach that infers the level of trust that takes into consideration context of C2C among users on Twitter to reduce uncertainty and the risk of fraud or scams on this social media platform. Applications will eventually access and utilize trust inference data incorporated into web-based social networks (Golbeck & Hendler, 2005).

1.3 Aim

The purpose of this research was to develop an algorithm that can infer the trust level among users engaging in consumer-to-consumer e-commerce on Twitter taking into consideration the context of the intended transaction.

1.4 Specific Objectives

- i. To investigate factors that are important for establishing trust in consumer-to-consumer e-commerce on Twitter.
- ii. To review existing models and algorithms used in consumer-to-consumer e-commerce sites to infer trust among consumers.
- iii. To develop an algorithm for inferring consumer-to-consumer trust on Twitter.
- iv. To validate the algorithm for inferring consumer-to-consumer trust on Twitter.

1.5 Research Questions

- i. What factors are important for establishing trust in consumer-to-consumer e-commerce on Twitter?
- ii. Which existing models and algorithms are used in consumer-to-consumer e-commerce sites to infer trust among consumers?
- iii. How can the proposed algorithm for inferring consumer-to-consumer trust on Twitter be developed?
- iv. How can the algorithm for inferring consumer-to-consumer trust on Twitter be validated?

1.6 Justification

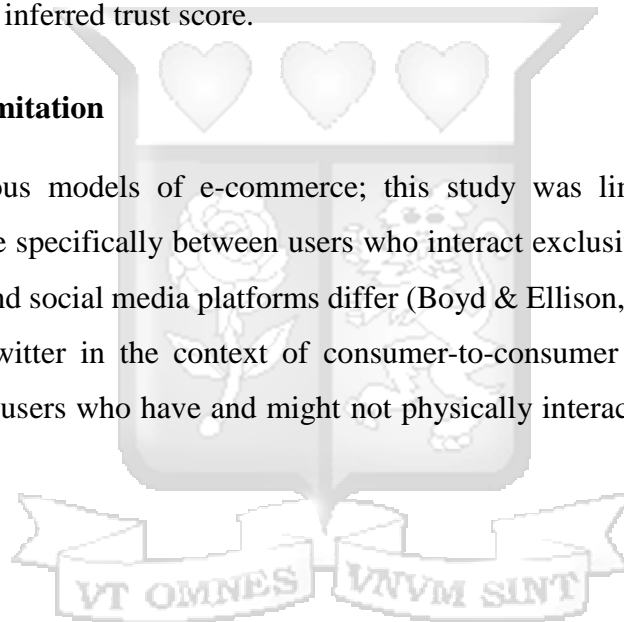
Communication is no longer about just businesses talking to anyone; it is about people talking to people. Individuals, whether buying for business or personal use, are talking to and listening to other consumers (Menzies, 2016). Trust therefore plays an important role when we need to determine who to engage in consumer-to-consumer e-commerce and on what especially

for users we have not met physically or face-to-face in the physical world. By assigning a set of trust scores and making them known to the users, a social media platform can both adjust how often and how far a message from a user spreads but also gives users incentives to behave better (Dignan, 2019). The algorithm will limit the extent to which a fraudulent seller messages and content can reach based on his/her trust score.

Social media platforms like Facebook-owned WhatsApp has limited the number of message forwards to five recipients to combat spam and false information from untrustworthy sources (Lackey & Graham, 2019). Slogans such as Alipay's "trust makes it simple" (Alipay, 2018), shows the significance of trust in C2C e-commerce. The algorithm proposes different trust scores to help consumers to accurately decide how to interact with other consumers on Twitter based on their inferred trust score.

1.7 Scope and Limitation

There are various models of e-commerce; this study was limited to consumer-to-consumer e-commerce specifically between users who interact exclusively on Twitter; this is because cultures around social media platforms differ (Boyd & Ellison, 2007). The focus is on analyzing trust on Twitter in the context of consumer-to-consumer e-commerce (Svec & Samek, 2017) among users who have and might not physically interact using C2C keyword-hashtag (#).



Chapter 2: Literature Review

2.1 Introduction

In this chapter, the focus is on the literature on consumer-to-consumer e-commerce business model; trust algorithms, feature selection and machine learning algorithms and how these algorithms have been applied in social media networks. A conceptual framework is then presented at the completion of the literature review.

The use of social media sites as consumer-to-consumer e-commerce platforms was the subject of our research. The role of social media in e-commerce is evolving. The opportunities for them to interact with and bolster each other are innumerable (Martin, 2017). Social media users are increasingly using the site to conduct commercial activities, by posting advertisements in groups and buying or selling items from each other (Chen, Su, & Widjaja, 2016). This phenomenon of using social media sites for C2C e-commerce is also referred to as social commerce (Chen, Su, & Widjaja, 2016). This emerging type social commerce allows any user on social media platforms to act as sellers or buyers on these platforms. Users can sell second hand items, run small retail shops, sell self crafted goods, offers personal services such as crowdsourcing among others (Bao & Volkovynska, 2016). Social commerce is a sub-category of e-commerce. Social media users just like companies are faced with the challenges posed by big data in this era of Industry 4.0. In today's competitive consumer-to-consumer e-commerce world, users are faced the challenge of making rapid decisions about large amount of data present on social media (Dignan, 2019).

2.2 E-Commerce Business Models

C2C e-commerce was previously only represented in online auction sites like eBay, Amazon, Craigslist among others. Consumers are now using social media platforms as C2C e-commerce sites (Chen, Su, & Widjaja, 2016). These sites facilitate the transactions and provide a platform for consumers to connect with each other.

Business models can be categorized based on the nature of transacting parties or between parties that are conducting business that is buying/selling of goods or services. According to Laudon and Traver (2014) e-commerce business models are as follows; business-to-consumer (B2C) that is, business formed between business and consumer. Business-to-business (B2B) e-

commerce is electronic transactions between companies. Consumer-to-business (C2B) is seldom practiced but is common in the world of arts, for example Shutterstock. Consumer-to-consumer (C2C) is the business model that facilitates commerce between private individuals. Whether it's for goods or services, this category of e-commerce connects people to do business with one another. C2C is the focus of this research. Others are Business-to-Administration (B2A) and Consumer-to-Administration (C2A).

2.3 Consumer-to-Consumer (C2C) e-commerce

Consumer-to-consumer e-commerce is a growing area of e-commerce, largely because of the growth of the Internet (Dan, 2014). Amazon and eBay are two prominent third-party C2C providers. C2C platforms has myriad of advantages such as providing convenience to users, some are free or charge a small amount as commission. C2C e-commerce has grown in leaps and bounds as they act as intermediaries matching buyers and sellers. C2C platforms have little control over the products and services sold on their platforms. They are only intermediaries for connecting consumers. They are not responsible for the product or service exchange. C2C platforms have a number of cons as well.

In C2C e-commerce, the consumers often do not have first-hand information for reference, in order to form trust in the seller, consumer use second-hand data and information made public in electronic platforms such as Twitter (Zhang, Chen, & Sun, 2010). Consumers need to know if they can trust the other party in a C2C transaction. Consumers spend a lot of time and effort on figuring out exactly that (asking for references, looking for more information on Google, running credit and background checks among others).

A consumer can be helped by social media community to make decisions (Baghdadi, 2013). Information disclosure by both the buyer and seller informs their level of trust amongst them. The unavailability of this kind of information creates uncertainty. C2C transactions may be one-time therefore the trust relationship between the buyer and sellers must be established before-hand (Zhang, Chen, & Sun, 2010). Information disclosure is a double edged sword as it introduces privacy concerns. Privacy and security will not be addressed by this research as it has been extensively discussed by other researchers.

Figure 2.1 shows the business model for C2C e-commerce.

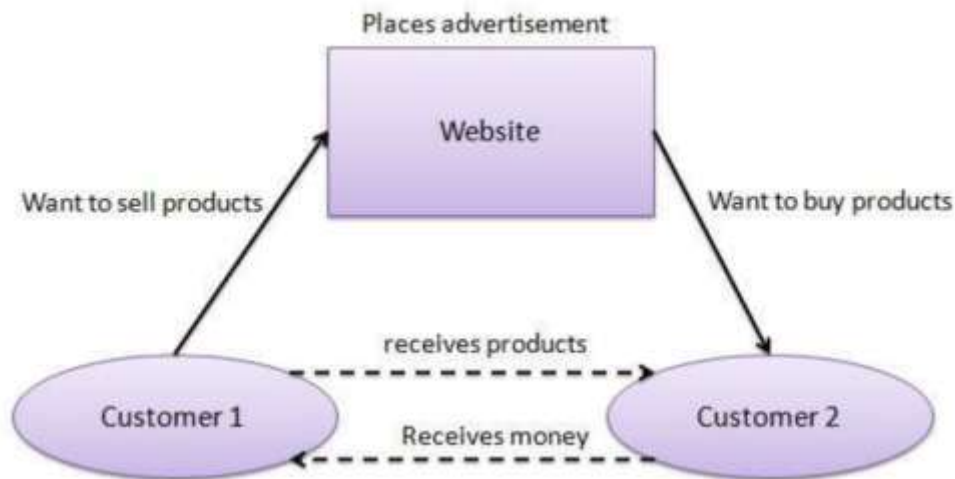


Figure 2.1 : C2C E-commerce Business Model (Rivera, 2018)

These platforms can be rife with scams; users can pay for products/services and have them delivered late, sub-standard or never at all (Dan, 2014). Products or services can also be sub-standard, defective or damaged. C2C platforms do not provide guarantees of the products/services. In C2C, the user can be both a seller and buyer. In C2C e-commerce on Twitter, users take on social activity first then turn to transaction activity later. According to the Communications Authority of Kenya (2018) report, there was an increase in online abuse in the third quarter of calendar year, 2018. Online abuse in this report includes online fraud; hate speech, incitement to violence and fake news on social media platforms.

2.4 Concept of Trust in Social Media

Trust is a social phenomenon. Trust is also closely related to risk. Trust is one of the most important components in e-commerce because of the high degree of uncertainty (Thaw & Mahmood, 2009). Trust is a subjective quantity calculated based on the two agents concerned in a dyadic encounter (Mui, Mohtashemi, & Halberstadt, 2002). Trust has been studied in many disciplines including sociology, psychology, economics, and computer science (Sherchan, Nepal, & Paris, 2013). Each of these disciplines has different definitions of trust.

Trust is a subjective expectation and differs among different people and researches. Trust can be defined in a number of ways. The Merriam-Webster Dictionary (2018) defines trust as assured reliance on the character, ability, strength, or truth of someone or something. Another definition is that trust is a measure of confidence that an entity will behave in expected manner, despite the lack of ability to control or monitor the environment in which it operates (Yu &

Guo, 2016). Two common ways of determining trust are through using policies or reputation (Artz & Gil, 2007). Also, trust in computer science, can be classified into two categories, user and system (Mui et al., 2003). In consumer-to-consumer e-commerce sites like Amazon and eBay, trust is based on the feedback on past interactions between members (Resnick & Zeckhauser, 2002).

Social interactions on Twitter are quickly becoming a concept that spans multiple geographical, political and cultural boundaries. The roles that trust play in the “physical” environment also applies to the social media (Abdul-Rahman & Hailes, 2000). Social media increases “social presence” through real-time interactions which increases trust in C2C e-commerce. Social presence is defined as “the extent to which a medium (social media) allows a user to experience others as being psychologically present” (Gefen & Straub, 2003).

The main differences between reputation and trust are that reputation is an objective concept that demonstrates a collective evaluation of individuals or companies whereas trust is a subjective concept that reflects an individual’s idea (Wang & Vassileva, 2007). Trust is gained through reputation and then through repeated experiences (Gustavsson & Johansson, 2006). The definition of trust that will be adopted in this research is the one proposed by Golbeck (2005), which is “trust in a person is a commitment to an action based on a belief that the future actions of that person will lead to a good outcome”.

2.5 Dimensions Determining Trust

According to Kim et al. (2017) and Corbitt et al. (2008), six dimensions determine trust in ICT, namely social, institutional, content, product, transactional and technological dimensions. Incorporating all aspects of trust introduces a large number of variables; this makes the model large and complex because trust itself is very complex and multi-faceted (Abdul-Rahman & Hailes, 2000). Reputation plays a key role in commerce, it is an important mechanism to build consumer trust, reduce transaction risk, and facilitate smooth transaction (Zhang, Chen, & Sun, 2010).

Techniques presented by Gustavsson and Johansson (2006) that can be used to promote trust on the Internet are marketing, education, trust seals, community, code, protection, and dispute resolution. Code is defined in this sense as a powerful mechanism for building trust underlying the social media site (Gustavsson & Johansson, 2006). The researcher’s argued that

users can use visible elements present in social media including Twitter to get an impression of the trustworthiness of the consumer.

2.6 Trust Metrics in Social Networks

Trust metrics compute quantitative estimates of how much trust an agent **a** should accord to its peer **b**, taking into account trust ratings from other persons on the social network (Ziegler & Lausen, 2005). Trust metrics can be divided into two scopes: global and local scopes (Ziegler & Lausen, 2005). Global trust metrics take into account all peers and trust links connecting them while trust metrics with local scope, take into account personal bias (Ziegler & Lausen, 2005). Trust concept can be divided into direct and recommender trust (Abdul-Rahman & Hailes, 2000). They represented direct trust as one of four agent-specified values about another agent (“very trustworthy”, “trustworthy”, “untrustworthy”, and “very untrustworthy”. Recommended trust can be derived from word-of-mouth recommendations, which they consider as “reputation”. The translation from recommendations to trust is performed through an ad-hoc scheme (Abdul-Rahman & Hailes, 2000).

Trust has been found to provide useful intuition for social media networks. Trust is gained through reputation and then through repeated experiences (Gustavsson & Johansson, 2006). Trust algorithms can be divided into two categories; global and local algorithms. Global algorithms try to compute a universal trust value for each person in the trust network. This trust value is called reputation. Local trust algorithms calculate trust values from the perspective of the person asking for the trust recommendation (Taherian, Amini, & Jalili, 2008).

On Twitter, interactions between users can be used to infer trust between two consumers. These interactions between consumers are expressed through a hashtag (#), based on this hashtag, a user’s profile can be mined and used in this research to infer trust. Twitter has various ways in which consumers can interact. First, a user can follow another user, second, a user can retweet another users tweets, third, he/she can favorite another users’ tweet and finally he can mention another user. Retweets and mentions express trust but to varying degree (Carrasco, 2012).

2.7 Properties of Trust

Trust has various properties. These properties of trust influence what kind of trust is being studied and modeled. According to Sherchan, Nepal, and Paris (2013) trust properties are classified as follows:

Dynamic – Trust is not static; it can increase or decrease with time, new experience, observation or interactions. (Staab & Engel, 2008). Good experiences lead to increase in trust while bad experiences decrease trust. Also, new interactions are considered more valuable than old ones for assessing the recent behavior of a seller (Zhang, Chen, & Sun, 2010).

Context specific – Trust should always be associated with a specific context (Staab & Engel, 2008). In this research, we will consider the context of the transaction for consumer-to-consumer e-commerce on social media specifically Twitter taking into account past user activities/interactions.

Propagative – Trust can be passed from one member of a social network to another, creating trust chains. It is similar as the “word-of-mouth” propagation of information for humans (Abdul-Rahman & Hailes, 2000).

Aggregative – Information from multiple sources is aggregated to form a final value for trust. Golbeck (2005) proposes a trust composition function based on the structure of trust relationship.

Subjective – Trust is subjective. The subjective nature of trust leads to personalization of trust computation, where preferences of the member have a direct impact on the computed trust review. This work will not be addressing this property of trust, as this research will be looking at a users activity/interaction on social media.

Asymmetric – Trust is asymmetric. User A might trust user B. However, user B might not trust user A. This is because of people’s difference in culture, perceptions, and opinions among others.

Event sensitive – Trust takes a long time to build. However, one high impact event might destroy it (Nepal et al., 2009). This property will not be the investigated in this research.

2.8 Trust Contexts

Context is always related to a certain situation. The Webster Dictionary defines context as “the situation in which something happens”. Therefore, the statement, “trust is therefore context dependent”, implying different circumstances require different considerations in regards to trust (Zhang, Chen, & Sun, 2010). In order to provide an accurate evaluation of a seller/buyer on Twitter for a specific context, the inference of trust needs to take into consideration the context. Context in this study refers to consumer-to-consumer trust on Twitter as a platform.

In consumer-to-consumer e-commerce, different transactions need to be assessed differently because these transactions are of a different nature and value. A seller on social media is to be considered differently with regards to his/her trustworthiness in other potential future interactions (Zhang, 2014). Consider a seller on Twitter selling a used laptop, the seller can be trusted by a buyer to be able to deliver the used laptop but might not be trusted to deliver a birthday cake. Here we see aspect of product category being taken into consideration. There are various combinations of context in relation to consumer-to-consumer trust on Twitter.

The following example is used to describe context in relation to consumer-to-consumer trust, “I trust a user with a longer history on Twitter than a user with a brief history”. Trust context as discussed by Svec and Samek (2017) are interaction time span, that is, the higher the duration between initial and latest interaction, the higher the trust a user is likely to have, even though there may be exceptions to this argument. For example, if a seller only started their Facebook account the day before they posted something to sell, they may be attempting to scam a buyer (Facebook, 2018).

Number of interactions, here the researchers used the term interaction to mean one-way communication, for example posts and comments among other indicators. Interaction regularity, the researchers implied that, it is natural for users to trust people they communicate with daily than people they seldom communicate with. Photo tagging was also seen as important in inferring trust among users. Photo tagging indicates a connection between people in the real world.

Parameters of trust context according to Zhang (2014), are category of product, amount of transaction and time of transaction. The researcher presented a trust vector comprising of these three major values and termed them “context dimensions”. These trust values could outline the trustworthiness of a social media user, which indicates his/her dynamic trustworthiness in different products, categories and any combination of them. For example, in crowdsourcing environments, contexts are mostly related to the task itself and accordingly influence the trust relation between a trustor and a trustee. A user who trusts a person in a programming task may not trust the person in a T-shirt design task. In addition, regarding the influence of the transaction amount, a trustor who trusts a person in a task with \$5 reward amount may not also trust the person in a task with \$50 reward (Ye, 2018).

2.9 Existing Approaches of Trust Computation

There exist various approaches in the computation of trust on social media or social networks. These trust evaluation models can be classified as network-based trust models, interaction-based trust models and hybrid trust models (Situm, 2014). Interaction-based approach will be adopted in this research to determine the trust score of a Twitter user who engages in consumer-to-consumer e-commerce.

Researchers have presented various algorithms and models for determining trust on social media. Hentschel et al., (2014) presented an algorithm to identify Twitter users others can trust to be regular Twitter users and not spam or fake accounts. The technique starts with an initial set of trusted users based on Twitter’s verified users and recursively includes other users the trusted users communicate with. The algorithm only starts when a verified user initiates a conversation; this does not relate to real life scenario especially in relation to C2C e-commerce. However, we borrow their argument that verified profiles can be considered trustworthy.

Researchers who conducted a survey on user and tweet trustworthiness assessment using Twitter as a case study categorized existing approached into two. These are feature-based and social graph based trust ranking respectively (Zhao, Hua, Lu, & Chen, 2015). Existing works in feature-based trust ranking generally classify tweets as either credible or not in relation to a target topic using credibility “features” of tweets; the researchers applied supervised learning in the approach. On the other hand, social graph based trust ranking infers trust information from social graphs (Zhao et al., 2015). The approach presented by this works is different from

the above cited works, in that, our supervised machine learning approach seeks assign a trust score to a Twitter user who engages in consumer-to-consumer e-commerce using select features on his/her Twitter profile. We further, utilize multi-class classification in our approach.

2.10 Trust Computation on Social Media

Certain features have a strong influence on a models ability to predict useful information in specific contexts (O'Donovan et al., 2012). Trust computation criteria employed by Twitter has taken various directions based on the context of the study. The most important feature on Twitter is “retweeting”, it is an action of repeating a tweet to one’s own followers (Anger & Kittl, 2011). The follower/following ratio known as the golden ratio is another important metric to measure influence on Twitter, it compares the number of users who have subscribed to user X updates with the number of users that user X is following. If the result is smaller than 1, the user is considered to have less influence (Anger & Kittl, 2011). To see an indication of how user X’s tweets are reacted to by the audience, the retweet and mention ratio is important. This shows that user X’s tweet lead to a communicative action with another user. Twitter has set mechanical limits to this ratio on all Twitter accounts to this ratio to limit fraudulent users, bots and spammers (Parsons, 2017).

A Twitter account, can only follow up to 5,000 user accounts, to follow more users, the number of people following a user should also reach or exceed 5,000 users (Parsons, 2017). Interaction time span is also an important element in the computation of C2C trust on social media. A user with a shorter interaction time span is considered less trustworthy (Facebook, 2018). Account authority features studied by Bodnar, Tucker, Hopkinson and Bilen (2015) concluded that retweets and mentions are good indicators of a user trustworthiness on social media.

2.11 Machine Learning Approach to C2C Trust on Twitter

2.11.1 General Trust Prediction Model

In this subsection, we discuss the general trust prediction model using machine learning techniques on Twitter. The first step is collection of the dataset from Twitter Search API. The second step is preprocessing of the raw dataset by selecting those quantifiable features that can be used to infer the trust score of a user. The quantifiable factors are then used to train machine learning models. Finally, the model is evaluated using various performance metrics. The

trained model with satisfactory performance can then be integrated to a number of real world applications. Figure 2.2 shows the pipeline for trust prediction based on machine learning techniques.

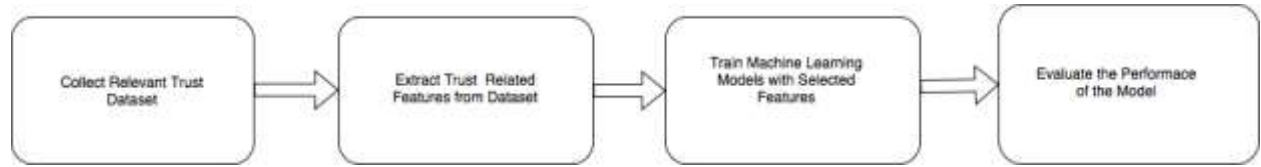


Figure 2.2 : Pipeline of Trust Prediction Models (Liu, Zhang, & Yan, 2018)

2.11.2 Feature Selection

Feature selection is generally used as a preprocessing step. The goal of feature selection is to choose a subset, X_s of the complete set of input features $X = \{x_1, x_2, x_3 \dots x_M\}$ so that the subset X_s can predict the output Y , accuracy comparable to the performance of the complete input set X , and with great reduction of the computational cost. (Jović, Brkić, & Bogunović, 2015). Feature selection is also called variable selection or attribute selection. One of the steps in this research is to identify Twitter profiles of users who have engaged in C2C e-commerce by purposively selecting tweets close associated with C2C e-commerce from other topics of discussion by users. Feature selection is the process where you automatically or manually select those features which contribute most to your prediction variable or output in which you are interested in (Shaikh, 2018). The benefit of performing feature selection before modelling data include reduction of over-fitting, improves accuracy and reduction of training time (Shaikh, 2018). Feature selection makes training and applying a classifier more efficient by decreasing the size of the effective vocabulary. This is of particular importance for classifiers that, unlike Naïve Bayes, are expensive to train. Feature selection often increases classification accuracy by eliminating noise features (Manning et al., 2008).

Different social media features are important in specific contexts (O'Donovan, Kang, Meyer, & Hollerer, 2012). The question posed by the researcher is “which features are best for inferring a users trust score on Twitter?”. In this research, we posed that instead of trying to determine which features infer the trust score of a user, this research concentrated on specific contexts that determine when specific features are useful in determining a user trust score. Features on Twitter have a diverse usage across different contexts. Certain features have a

strong influence on a models ability to predict useful information in specific contexts (O'Donovan et al., 2012).

Azab, Idrees, Mahmoud and Hefny (2016) proposed a minimum of seven (7) Twitter features and weights that can be used to detect fake accounts. Various researchers have used various features to detect fake accounts on Twitter (Benevenuto, Magno, Rodrigues, & Almeida, 2010; Stringhini, Kruegel, & Vigna, 2010). Zhao et al., (2015) posed that some Twitter features can be used as an indicator of a Twitter users trustworthiness. They singled out, account length time (time since joining Twitter), favourite count, follower count, following count, list count (categories of interest to the user) and whether account is verified or otherwise. Since most users on Twitter are not verified, this research will only seek to determine trust amongst unverified users. Verified users will be assumed to be trustworthy (Zhao et al., 2015).

Research has shown that Twitter features can be used to measure a user influence on Twitter. Building upon this research, our research seeks to assign a consumer a trust score under the context of consumer-to-consumer e-commerce on Twitter. This study utilized a hashtag (#) to identify users who have engaged in C2C e-commerce. A hashtag (#) is a word or a collections of words proceeded by the symbol (#) and concatenated together with underscores or using a upper-lower case convention (Twitter, 2019). Hashtags carry various semantic meaning and associations including C2C e-commerce association in a tweet, this study explored this component of Twitter. Spam hashtags targeting popular hashtags from spammers and bots have been on the increase, at the same time, intelligent optimization algorithms employed by social media platforms makes it easy for users to interact with social media (Maff, 2018).

Feature selection is therefore an important preprocess for any multi-classification process. The next section discusses popular feature selection methods. These methods are used to identify which attributes need to be considered from the various features present.

2.11.3 Filter Approach

This approach is based on statistics; it looks at the features and assigns a score to each. The features based on scores are either selected or removed from the dataset. The methods are mostly of one variable and usually consider the features independently, or with regard to the dependent variable. This means that the filter approach does not account for interactions

between features. Chi squared test, information gain and correlation coefficient scores are examples of this approach. (Sánchez-Marño, Alonso-Betanzos, & Tombilla-Sanromán, 2007). Figure 2.3 describes filter-based feature selection.



Figure 2.3 : Filter-Based Feature Selection (Kaushik, 2016)

2.11.4 Wrapper Approach

This approach creates a rank based on metrics derived from the measurement algorithm. This approach allows for fair comparison between different algorithms. Since it guarantees optimal feature combination on a per algorithm basis, it eliminates any bias in the analysis due to poor selection. Wrapper methods measure the usefulness of features in classification algorithm. It picks up possible combinations of features and chooses the combination with the best results for a particular classifier model. Its disadvantage is that it tests all possible combinations of available features, which is expensive to compute, especially if the feature set is big (Sánchez-Marño et al., 2007). Figure 2.4 describes wrapper-based feature selection.

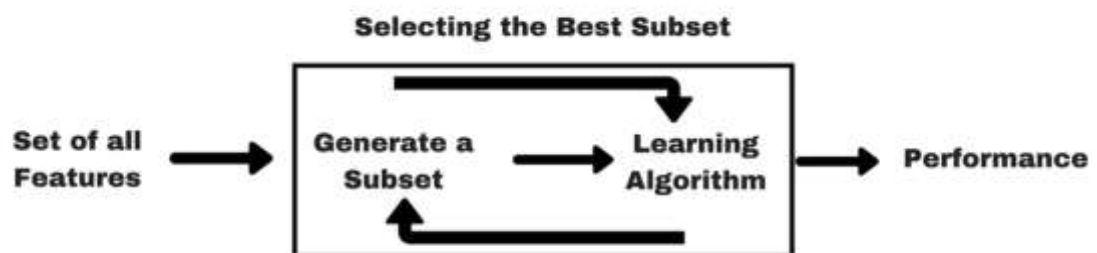


Figure 2.4 : Wrapper Feature Selection (Kaushik, 2016)

Wrapper methods for feature selection can be divided into three categories: step forward feature selection, step backwards feature selection and exhaustive feature selection. For step backwards feature selection, one feature is removed in round-robin fashion from the feature set and the performance of the classifier is evaluated and is the inverse of step forward feature selection. In exhaustive feature selection, the performance of a machine learning algorithm is

evaluated against all possible combinations of the features in the dataset. (Sánchez-Marono et al., 2007).

2.11.5 Hybrid Approach

The hybrid approach was proposed as a combination of the best properties of the filter and wrapper approach discussed previous two sub-sections. The filter approach is used to feature space dimension space and possibly obtaining several candidate feature subset. The wrapper technique is the used to find the best candidate subset (Jović, Brkić, & Bogunović, 2015). The wrapper technique has the combined benefits offered by both approach with high accuracy derived from wrapper and high efficiency of the filter technique.

From the above approaches presented, the wrapper approach has been singled out because it allows for a fair comparison between different algorithms. The wrapper technique provides for the best feature combination that will be adopted for this research, it selects features on a per algorithm basis, therefore eliminates any bias because of poor selection.

2.12 Machine Learning (ML) Algorithms

We analyze machine learning models mostly used in trust inference in this section. Classification is used to find out in which group each data instance is related within a given dataset. It is used for classifying data into different classes according to some constrains. Several major kinds of classification algorithms including Decision Trees, Random Forest, K-Nearest Neighbor, Neural Networks, Bayesian Classification, and Support Vector Machines are used for classification. Generally a classification technique follows three approaches Statistical, Machine Learning and Neural Network for classification (Manning et al., 2008). In order to infer the trust score of a social media user using selected features on his/her profile, the model employed a classification machine learning technique. The next sub-section describes the various machine learning algorithms employed by this study. Table 2.1 compares commonly used classification algorithms for inferring trust in social media.

Table 2:1: Comparison of Typical Classifiers (Liu, Zhang, & Yan, 2018)

Classifier	Advantages	Disadvantages
Decision Tree	Handles discrete or categorical features well; no parameters tuning	Incorporate new instances is hard; performances badly on imbalanced datasets
KNN	No parameters tuning	Requires a large space for storage; its feature selection requirement is high
Naïve Bayes	Converges quickly; high accuracy even for small datasets; incorporation of new instances is easy	Only work on discrete features
SVM	Its complexity is independent of the number of applied features	Require large training datasets

2.12.1 Decision Tree

Decision tree algorithm can be used for both classification and regression purposes (Manning et al., 2008). The most common decision trees algorithms are Iterative Dichotomiser (ID3), C4.5 and CART (Han et al., 2012). Decision tree is one of the most widely used classifiers in statistics and machine learning. Decision tree is a hierarchical design that implements the divide-and-conquer approach. It is a nonparametric technique used for both classification and regression. It can be directly converted to a set of simple IF-THEN rules. It's straightforward representation makes the reader able to interpret the result and easy to understand (Mohamed, 2017).

Decision tree algorithms adopt a greedy approach. It simple and splits at the nodes. It has both nodes and terminal leaves. At each node, a test function is performed to make a decision on which branch or the leaf is chosen, which means that the decision of the class that the instance belongs to. The process starts at the root; where a decision is made at each node al the way to the leaf. The predicted class of the given example will be its label (Alpaydin, 2014).

2.12.2 Random Forest

Random forest is part of a collection of decision trees. The trees built in Random forest are based on majority voting, which is already a representation of an accurate output. In Random forest, cases in the training dataset will be sampled randomly but with replacement from the original data. This sample will then act as training set for growing the tree. In order to split the nodes, a constant value is chosen during the entire growth of the tree. Each tree is made to grow to the largest extent possible. (Manning et al., 2008). Random forests can be built using bagging in tandem with random attribute selection and Classification And Regression Trees (CART) methodology is used to grow the trees. Bagging works as a method of increasing accuracy (Han et al., 2012).

2.12.3 Support Vector Machines

Support Vector Machines (SVMs) is a supervised learning algorithm, focused as a predictive multiclass classifier suggested for the first time by Vapnik (1998). This supervised algorithm is used for both classification and regression problems. A classification has a discrete output while regression has a real number as its output (Mohamed, 2017). Most researchers and scientist mostly prefer this algorithm as it produces significant accuracy with less computation overhead. The objective of the SVM algorithm is to find a hyper-plane in an N-dimensional space (N—the number of features) that distinctly classifies the data points (Mohamed, 2017).

2.12.4 Naïve Bayes

Naïve Bayes is a simple, yet effective and commonly used, machine learning classifier. It is a probabilistic classifier that makes classifications using the Maximum A Posteriori decision rule in a Bayesian setting. It can also be represented using a very simple Bayesian network. Naïve Bayes classifiers have been especially popular for text classification, and are a traditional solution for problems such as spam detection (Mohamed, 2017).

2.12.5 K-Nearest-Neighbor (KNN)

KNN algorithm is based on the assumption that like items exist in close proximity (Mohamed, 2017). KNN finds the distances between an object in question and all the examples in the data, thereby selecting the number of examples (K) closest to the question, then chooses for the most frequent label (for classification) or averages the labels (for regression) (Hassanat, Abbadi, Altarawneh, & Alhasanat, 2014). The KNN classifier is one of the most popular neighborhood classifiers in pattern recognition and, because the technique is very simple, and highly efficient in the field of pattern recognition, machine learning, text categorization, data mining, object recognition (Hassanat et al., 2014).

To determine which of the K instances in the training dataset are most similar to a new input a distance measure is used. For real-valued input variables, the most popular distance measure is Euclidean distance (Mohamed, 2017). Other popular distance measures include Hamming distance, Manhattan distance and Minkowski distance. This research is going to utilize Euclidean distance as a distance measure.

2.13 Conceptual Framework

The researcher proposes a conceptual framework to infer a trust score for a social media user who engages in C2C e-commerce using selected features for a specific context. The user's profile data will be mined from Twitter based on C2C keyword-hashtag to create the corpus to be used for training the model. The researcher will apply wrapper method for feature selection because of the benefits outlined in literature. The contribution of the selected features will be looked at individually and later, all features combined. The researcher will then use the selected features to train various machine learning classifiers such as Random Forest and KNN to learn the model for inferring the trust score of a user from the training set.

In this study, the researcher will be interested in the classifier performance of the selected models as a measure of their performance in predicting the trust score of a given Twitter user.

Based on the literature review, the conceptual framework in Figure 2.5 is proposed.

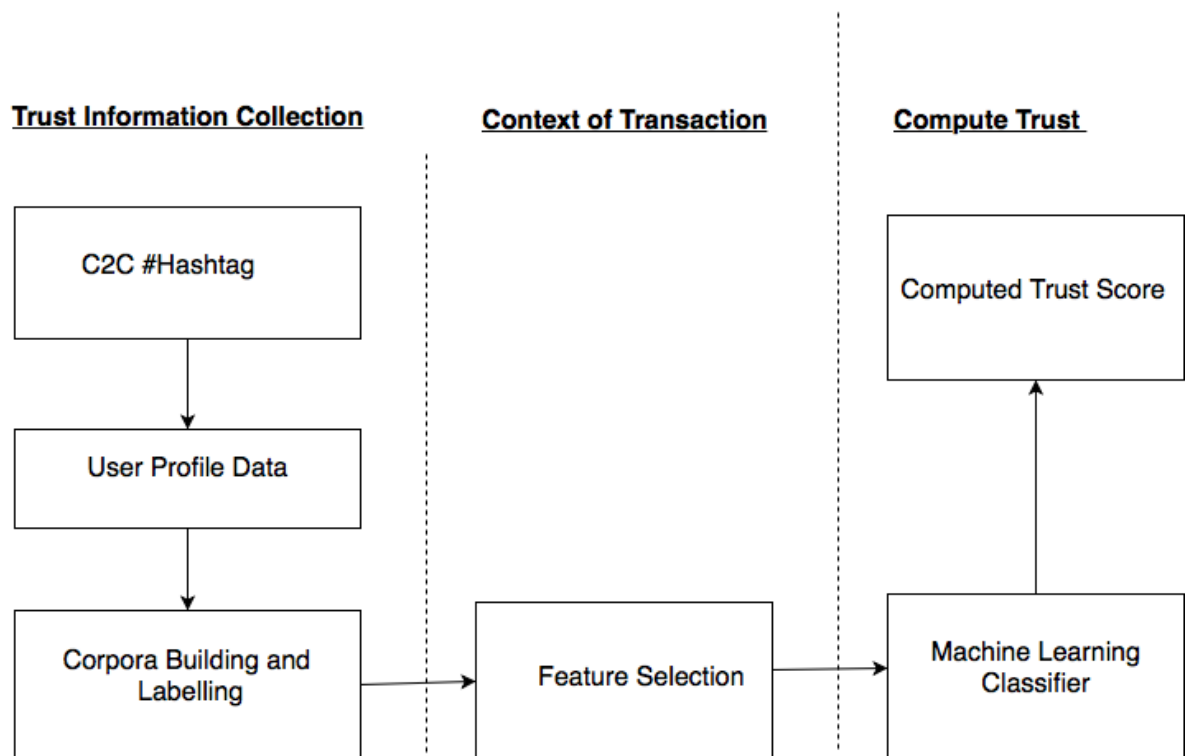


Figure 2.5 : Conceptual Framework



Chapter 3: Research Methodology

3.1 Introduction

This chapter presents the methodology employed for data gathering as well as the relevant statistical analytical tools that were employed for analyzing the results gathered during this study. Research methodology is concerned with how research should be conducted (Saunders, Lewis, & Thornhill, 2009) and is usually philosophical in its approach (Fisher, 2007), it involves social and natural sciences (Bryman & Bell, 2011). The term method can be used interchangeably with technique; and also with procedures used to obtain data (Saunders, Lewis, & Thornhill, 2009).

3.2 Research Design

Research can be approached from different perspectives depending on the relationship between theory and research. Research approach can either be deductive or inductive (Bryman & Bell, 2011). A deductive approach is concerned with the development and the testing of theory while the inductive design is more concerned with understanding humans and their interpretation of their social world (Bryman & Bell, 2011). This research took an inductive approach, in the sense that the data was collected, analyzed, and finally a conceptual model developed. Also, this research took an experimental design approach, which involved the identification of research objectives, development of an algorithm and validation of the algorithm using a number of experiments to ensure the best performance (Creswell, 2009).

3.3 Population and Sample

The target population were users on social media platforms specifically Twitter who have engaged in consumer-to-consumer e-commerce. Purposive sampling was used by the researchers who choose their samples based on select features that can directly contribute to a deeper understanding of the phenomenon they are studying (Bryman, 2016). A random sample of Twitter user profiles that have engaged in consumer-to-consumer e-commerce were purposively sampled based on their tweets (using keywords) relating to specific context related to this study. To limit our sample to users who have engaged in C2C e-commerce on Twitter, we used a hashtag (#) that is strongly associated with C2C e-commerce. The hashtag (#) #IkoKaziKE, a Swahili word that translates to “there is work in Kenya”, was used to identify

users who have engaged in C2C e-commerce. The main entity in a tweet that was considered in this study was a hashtag (#) that related a tweet to C2C e-commerce context.

3.4 Data Collection Instrument

One of the methods used for data collection was data mining. Data mining was used to collect data on Twitter profiles using C2C e-commerce keywords specifically hashtag (#). The data collected formed the corpus used in this research. A domain expert performed manual annotation of the collected user profiles; a user was assigned a trust score for a specific context. Based on literature reviewed and input from domain experts, a judgement matrix was developed and adopted for assigning trust scores to Twitter users who have engaged in C2C e-commerce. The annotated data was then used as the ground truth for classification of a user on Twitter for the context under consideration (Vedula, Parthasarathy, & Shalin, 2018).

The ground truth approach adopted in this work is an approach used in statistics and machine learning to gather proper objective data for a test. The idea behind the ground truth approach is to collect proper objective data on the modeled trust score calculation and compare the result obtained from the evaluated algorithm with the result found in ground truth data (Smailovic, Podobnik, & Lovrek, 2018). In other related research, the ground truth data was collected through questionnaires where the number of social media users determined the level of trust between a user and other social media users (Smailovic et al., 2018).

3.4.1 Mining Twitter

Twitter was used to gather the primary data from purposively sampled Twitter users based on C2C keyword-hashtag (#) in tweets that are associated with consumer-to-consumer e-commerce was used for this research study. We mined data from Twitter using Twitter Search API through the TwitterR package of Exploratory software to get the tweet data based on C2C keyword-hashtag (#) search query. Samples of selected features are shown in Table 3.1 extracted from Twitter and analysed.

Feature selection was performed for each variable to better understand its contribution to the proposed model using wrapper approach. Each variable evaluated using wrapper approach using Scikit-learn package (Scikit-learn, 2019). A better understanding was sought, between the selected features and how can they (if they can) infer the level of trust amongst users who engage in consumer-to-consumer e-commerce. The collected tweets were 10,627. Table 3.1

shows information that will be retrieved using Twitter’s Search API, the JSON output includes a large amount of metadata features used for the algorithm (Twitter, 2019). In the dataset, the each row contains the following properties:

Table 3:1 Sample of Selected Features

No.	Twitter Feature	Feature Description	Feature Field Type
1.	User_id	String representation of the unique identifier for this user	Integer
2.	Entity	Entity which have been parsed out of the text of the tweet specifically hashtags (#)	Text
3.	Favourites	Number of favourites by the user	Integer
4.	Status_count	The number of Tweets (including retweets) issued by the user	Integer
5.	Followers_count	The number of followers this account currently has.	Integer
6.	Friends_count	The number of users this account is following (AKA their “followings”)	Integer
7.	Retweet_count	Number of times a Tweet has been retweeted	Integer
8.	Created_at	The UTC date/time that the user account was created on Twitter.	Date

The below steps describe the steps used for collecting tweets using Exploratory software. Figure 3.1 shows how to import Twitter search data with Exploratory software.

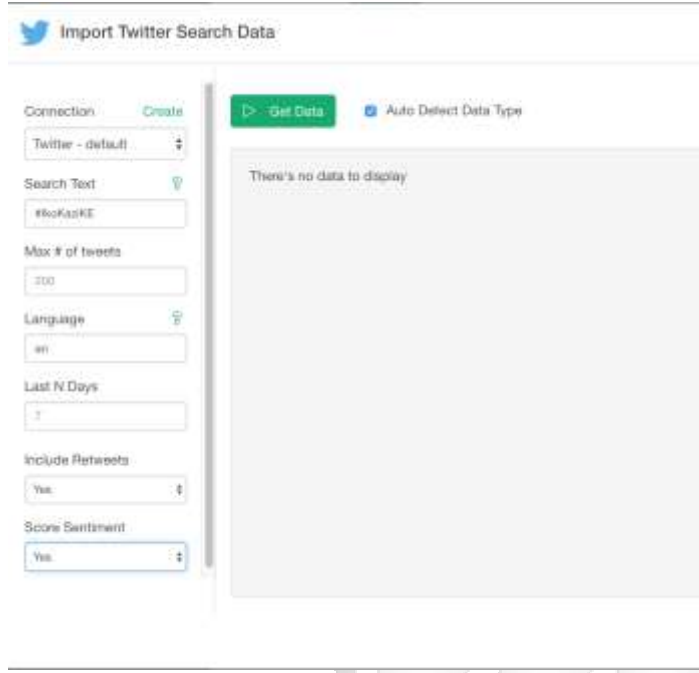


Figure 3.1 : Importing Twitter Search Data

3.5 Data Preprocessing

Data preprocessing is a data mining technique that involves transforming raw data into a format suitable for further processing in machine learning techniques. Noise removal is a part of preprocessing that has to be performed. To assign a user a trust score, the algorithm performed feature selection as part of preprocessing to select trust features. Features are metrics that characterize a user in some form such as number of followers, date of account creation among others. To select the features used by the algorithm, the model used the wrapper technique and Twitter Search API. The features that are used in this research are explained in section 3.4.1 in detail.

3.6 Model Training

The computation of a trust score for a consumer is presented in the form of a multi-classification problem. For training, the model used a known dataset. In this research, we will consider a user, u_k as identified by some select features, X_{u_k} , mined from the user's profile, who has been assigned a trust score, t_M as per the judgment matrix developed by a domain expert. Each user is uniquely identified by Twitter's *User_id* parameter. In the classification stage, each user, \hat{u}_k for which the trust score is not known, is assigned a trust score based on the learnt model. The collected dataset was randomly split into training sets (70%) and testing sets (30%), to be used to train and validate the model respectively.

3.6.1 Feature Weighting

One of the most challenging tasks in this research was encoding the notion of trust in some numeric form (feature weights). Liu et al. (2018) acknowledged that the assignment of feature weights is still being addressed by researchers, therefore continues to attract their attention. A simple strategy proposed by researchers is to learn encoding either through regression or classification from a labeled set of specific interactions and their associated weights obtained from a domain expert. Subsequently, we use the learned model to categorize the trust scores associated with other users within the social network (Vedula et al., 2018). We adopt the multi-class classification approach in this research. The features used for training the model can be broadly categorised as static and dynamic as shown in Table 3.1.

Feature weights from an offline model built using a judgment matrix model are then applied to generate trust scores. The model allows for weights to be assigned to specific feature combinations, this way the models can be adjusted to changes in each of the dimensions. For example, the weights assigned to features that represent a retweet action may have a higher weight than a favourite action, all other dimensions being the same. Similarly a retweet action by a user who has more followers than the user himself may have a higher weight than the same retweet action from one of the user's followers with a following less than theirs (Rao et al., 2015).

The judgement matrix approach adopted in this works was presented by Alrubaian et al. (2018). Using a domain expert to generate a judgement matrix concerning the importance of each feature. This was done once in the process of feature weighting. The judgement matrix, λ takes the form of a vector as shown in Equation 3.1.

$$\lambda = \begin{bmatrix} 1 & \cdots & f_{1n} \\ \vdots & \ddots & \vdots \\ f_{n1} & \cdots & 1 \end{bmatrix} \quad \text{Equation 3.1}$$

Pairwise comparison method is used to determine the relative importance of the selected features, which were evaluated on a numeric scale from 1 to 9. Pairwise comparison matrices are used in Multi-Attribute Decision problems (MADM) in order to express the preference of the decision maker (Bozóki, Dezsó, & Temesi, 2013).

3.7 System Development Methodology

The prototype to validate the algorithm will be developed following the Rapid Application Development (RAD) system development methodology that emphasizes on creation of applications in a short amount of time, sometimes with compromises in usability, features and execution speeds (Naz & Khan, 2015). Developed by James Martin, RAD accelerates the cycle of development of an application, resulting in the building of quality products faster and consequently saving valuable resources.

3.7.1 Overview of RAD Structure

The RAD phases and tasks involved in each stage can be depicted diagrammatically as in Figure 3.2.

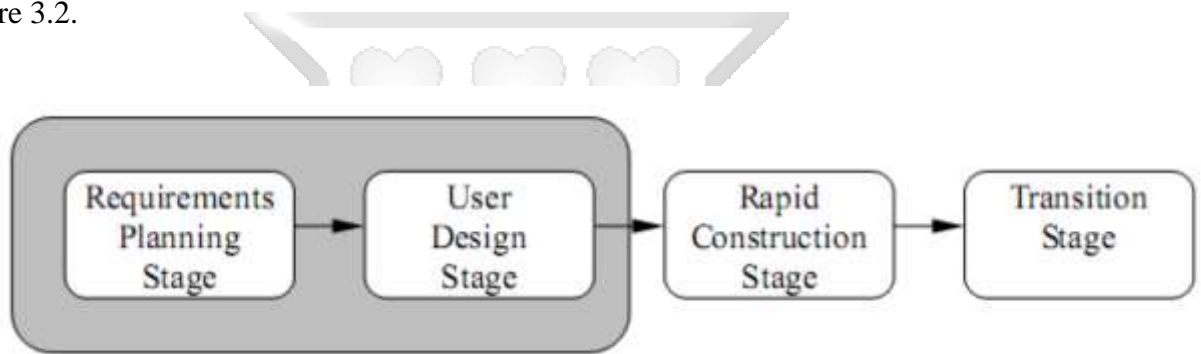


Figure 3.2 : RAD Life Cycle Stages (Orawit, 2006)

3.7.2 Phases of RAD

3.7.2.1 Requirements Planning Phase

The objectives of the Requirements Planning (RP) stage are: to establish a general understanding of the consumer and business problems related to consumer-to-consumer e-commerce on social media in specific contexts; there existing mechanism applied by social media provider to possible fraudulent consumers on social media is binary i.e. banned or not by the social media provider; trust is an important business component in C2C e-commerce on social media especially among users who have not met physically that lies in a wide spectrum and not just binary. The algorithm can therefore infer a consumers trust score that can be relied upon by other consumers to make a decision on how to engage with other consumers on social media.

3.7.2.2 Design Phase

The design phase produces a detailed system area model, an outline system design, and an implementation plan. Use cases, context diagrams, Data Flow Diagram (DFD) and sequence diagrams are designed at this stage to give a diagrammatic representation of the design.

3.7.2.3 Construction Phase

The application was developed using Python's scikit-learn library. Scikit-learn comes with various modules that can be used to implement various machine learning algorithms. The Pandas library was used because of its ease in handling data structures and data analysis (Panda, 2019). Another library used was, NumPy library, which provides useful features for operations on n-arrays and matrices in Python. For visualization, Matplotlib was used. Feature selection was implemented as a pre-processing step before the learning stage, scikit-learn Recursive Feature Elimination (RFE) was utilized as per Figure 3.3.

```
clf = Pipeline([
    ('feature_selection', SelectFromModel(LinearSVC(penalty="l1"))),
    ('classification', RandomForestClassifier())
])
clf.fit(X, y)
```

Figure 3.3: Sklearn Feature Selection Code Snippet

3.7.2.4 Transition Phase

The application was used to assign a trust score to a consumer on social media. The performance of the application was then monitored to see areas of improvement.

3.8 Validity and Reliability

Reliability and validity are important to provide a robust research design in any study. There exist four types of validity which are internal validity that determines the extent of drawing causative conclusions, external validity determines the extent of data generalization, statistical conclusion validity determines the appropriateness of the statistical methods used and their desired effects, and construct validity which determines constructs implemented successfully in the conceptual framework. In respect to the proposed study, the emphasis will be placed on construct validity.

Reliability refers to the capacity of measurement to produce consistent results (Sarantakos, 2013). He argues that a method is reliable if it provides the same results whenever repeated, and is not sensitive to the researcher, the research conditions or the respondents.

3.9 Ethical Consideration

According to Bryman and Bell (2007) some of the ethical considerations in research include prioritization of the respect and dignity of participants, obtaining consent, respecting the privacy of the research participants, declaring conflict of interest among others. The researcher used publicly available Twitter data therefore user permission was not required. The approach to obtaining and analyzing the Twitter data was in compliance with Twitter's terms of service at the time of the study.

3.10 Research Evaluation

Performance evaluation metrics are important in the effective performance of a classifier during training. Cross-validation was applied to split the data set into training and testing sets. The 10-fold cross-validation was specifically utilized in this research as it is good and can compromise between robust performance and being computationally less intensive and avoids overfitting (Scikit-learn, 2018).

The Confusion Matrix is a means to visualize the per class prediction performance of the model. The confusion matrix is of the form (true class, predicted class) where the rows represent true class and columns represented predicted class. Therefore we can infer that correctly classified points are grouped corresponding to the classes in the diagonal entries of the confusion matrix. The Confusion Matrix introduced by Kohavi and Provost (1998) is a method used to represent the classification performance of machine learning algorithms for attributes selection, as shown in Table 3.2.

Table 3:2 : Confusion Matrix

		Predicted Trust Score				
		Class A	Class B	Class C	Class D	Class E
Actual C Score	Class A	Accurate				
	Class B		Accurate			
	Class C			Accurate		

	Class D				Accurate	
	Class E					Accurate

Table 3.2 presents a confusion matrix for a multi-class classification, which is related to our research. This matrix allows researchers to identify, which points were correctly classified and which were not. A sample at M_{ij} where $i = j$ indicates the true class and predicted class are the same thus representing an accurate classification (diagonal positions). A sample that goes into M_{ij} where $i \neq j$ indicates that the true class i and predicted class j are not the same thus representing a misclassification.

Other parameter of evaluation like accuracy, precision, recall and F-measure, can easily be calculated from a confusion matrix are discussed in the next sub-section. The key used for the next section is as follows: TP – True positive, FP – False Positive, TN – True Negative and FN – False Negative.

3.10.1 Accuracy

A common measure for classification performance is accuracy, or its complement error rate. Accuracy is the proportion of correctly classified examples to the total number of examples, while error rate uses incorrectly classified instead of correctly. Equation 3.2 shows the formula for calculating accuracy based on confusion Table 3.1 (Manning et al., 2008).

$$Accuracy = \frac{(\text{correctly classified points})}{(\text{total number of points})} \quad \text{Equation 3.2}$$

3.10.2 Precision

Precision is used to measure exactness. Equation 3.3 shows the formula for calculating precision (Manning et al., 2008).

$$Precision = \frac{tp}{tp + fp} \quad \text{Equation 3.3}$$

3.10.3 Recall

Recall is shown in the Equation 3.4 (Manning et al., 2008). It shows the number of instances correctly labeled as positive over the total number of instances that are positive.

$$Recall = \frac{tp}{tp + fn} \quad \text{Equation 3.4}$$

3.10.4 F-Measure

Equation 3.5 shows how F-Measure is calculated (Ye, 2018).

$$F - Score = 2 * \frac{Precision * Recall}{Precision + Recall} \quad \text{Equation 3.5}$$

3.11 Model Validation

To validate the researcher's approach, a number of experiments were used to determine if the best combination of selected feature and machine learning algorithms were used to train the model for inferring the trust score of a social media user. To prove the validity of the proposed algorithm, we developed a model to assign trust score based on selected features.

Chapter 4: System Design and Architecture

4.1 Introduction

This research developed an algorithm for inferring consumer-to-consumer (C2C) trust on Twitter. Based on this objective, this section outlines the various requirements to be provided for by the proposed algorithm.

4.2 Requirement Analysis

The algorithm infers a trust score of a consumer based on selected features that are relevant for the context under investigation on Twitter. This section outlines the various requirements to be provided for by the proposed solution.

4.2.1 Functional Requirements

The following functional requirements were to be incorporated to the solution proposed.

- i. The application should capture the keywords-hashtag (#) to be used as context parameters in the retrieval of a consumers Twitter profile using the search function.
- ii. The application should retrieve the user's profiles from Twitter using the Twitter Search API matching the keywords-hashtag (#) specified by the consumer.
- iii. The application should perform feature selection of the retrieved profile and store them in csv format. The features selected should be the same as those used in training the model.
- iv. The application should assign a trust score trust score to a consumer using the proposed algorithm based on the machine learning models already trained.

4.2.2 Non-Functional Requirements

4.2.3 Usability

The intended users of the proposed application are social media users who intend to engage in consumer-to-consumer e-commerce on Twitter.

4.2.4 Scalability

The application should be scalable to other social media platforms such as Facebook since a user's online persona typically spans multiple social platforms. Also, the application should be able to handle a large number of users since social media users are always increasing.

4.2.5 Storage

The application should permanently store the trust scores for consumers that can be used to further train the model to make correct predictions from the dynamically collected data.

4.3 Proposed Algorithm

In order for the algorithm to determine consumer-to-consumer (C2C) trust score on Twitter, there is need to develop an algorithm for determining features present on Twitter that could be used to infer the trust score of a consumer. The researcher considered a number of user profiles, U_i as per Equation 4.1.

$$U_i = \{U_1, U_2, U_3, \dots, U_M\} \quad \text{Equation 4.1}$$

Where;

U_i is a consumer's Twitter profile.

Each consumer profile, U_i is characterised by a finite set of features as the trust features, $X_c^{U_k}$ for a specific context as per Equation 4.2.

$$X_c^{U_k} = \{X_c^{U_k}_1, X_c^{U_k}_2, X_c^{U_k}_3, \dots, X_c^{U_k}_R\} \quad \text{Equation 4.2}$$

We therefore, consider M , number of users, each represented by means of R selected features for a specific context. The goal of the proposed algorithm is infer the trust score, T , for each user, U_i for a specific context. Equation 4.3 shows the set of trust scores for users.

$$T = \{t_1, t_2, t_3, \dots, t_M\} \quad \text{Equation 4.3}$$

Where T is the trust score of a user for a specific context based on the selected features. We make the assumption that each user, u_k maps to a unique trust score, t_M . The assignment of

a trust score was framed in terms of a multi-class classification problem as earlier discussed. A user, whose trust score was not yet known, was assigned a trust score based on the learnt algorithm using machine learning techniques. The output of our proposed algorithm is a vector of the form shown in Equation 4.4.

$$T_u = \{X_c^{U_k}_1 \cdot w_1, X_c^{U_k}_2 \cdot w_2, \dots, X_c^{U_k}_R \cdot w_n\} \quad \text{Equation 4.4}$$

Where w_n is the weight vector based on λ , the weight vector assigns different weights to different features based on its importance in the context under consideration. The weight vector is applied to the selected features to generate the trust score of an unknown user, \hat{u}_k who will be assigned a trust score, t_M and so forth.

Table 4.1 shows the description and proposed selected features for the proposed algorithm. The features selected are those that change infrequently or those that change gradually. These features are those that are found in a user's account and cannot be changed by the user at will (Perez, Musolesi, & Stringhini, 2018). These features are static e.g. *Created_at* while others are dynamic features e.g. *Followers_count*. The algorithm will therefore take into consideration both static and dynamic features. The *User_id* feature is unique for each user profile.

Table 4.1: Description of Selected Features Based on Profile

No.	Twitter Feature	Feature Description	Feature Field Type
1.	User_id	String representation of the unique identifier for this user	Integer
2.	Favourites	Number of favourites by the user	Numeric
3.	Status_count	The number of Tweets (including retweets) issued by the user	Integer
4.	Followers_count	The number of followers this account currently has.	Integer
5.	Friends_count	The number of users this account is following (AKA their "followings")	Integer

6.	Retweet_count	Number of times a Tweet has been retweeted	Integer
7.	Created_at	The UTC date/time that the user account was created on Twitter.	Date

Table 4.2 presents the proposed algorithm to be used for calculating trust based on a consumer's Twitter profile.

Table 4.2: Pseudocode of the Proposed Algorithm

An Algorithm for Inferring Consumer-to-Consumer Trust on Twitter	
Input: Consumer Twitter Profile	
Output: Computed Consumer Trust Score	
<ol style="list-style-type: none"> 1. Fetch consumer Twitter profile metadata using C2C keyword-hashtag 2. Load profile features for consumer. 3. Select trust features relevant to the context 4. Load judgement matrix, λ 5. Return trust score of a consumer, T^{U_k} 6. End procedure 	

4.4 System Architecture

The system architecture shows the layout of the application implementing the algorithm for inferring the trust score of a C2C e-commerce user and the components it is made up of as illustrated in Figure 4.1. We use supervised machine learning techniques for assigning a trust score to a consumer using Twitter for C2C e-commerce. These techniques use training and testing datasets for Twitter users and select features that characterize those consumers. We used classification and created a model that combines different combination of the selected features. The keywords input by the consumer will be context of evaluating a user's trust score in a particular scenario. The Twitter Search API collects the profiles of the user's matching the user's keywords from Twitter Search API and stores them in user profile database. The pre-annotated dataset of users will be used to train the model. The model assigns a trust score to a user based on the classifier.

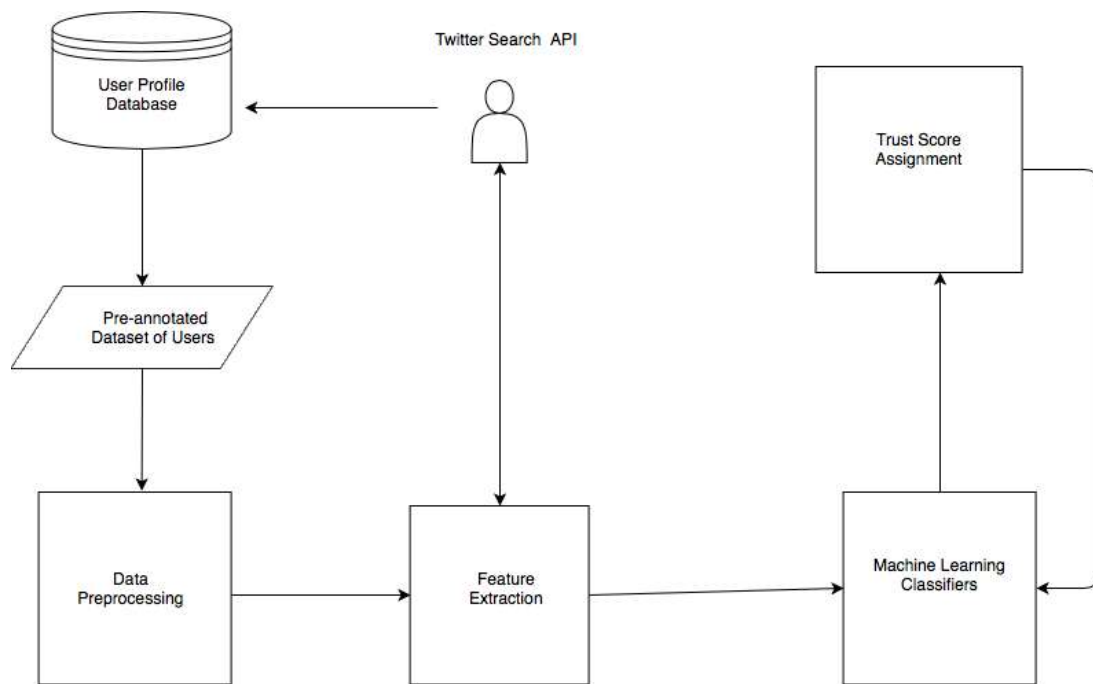


Figure 4.1 : System Architecture

4.5 Diagrammatic Representation of the Algorithm

4.5.1 Use Case Diagram

This diagram illustrates the list of actions or use cases that the algorithm fulfills. Use case diagrams are used to illustrate interaction between actors and the system as shown in Figure 4.2.



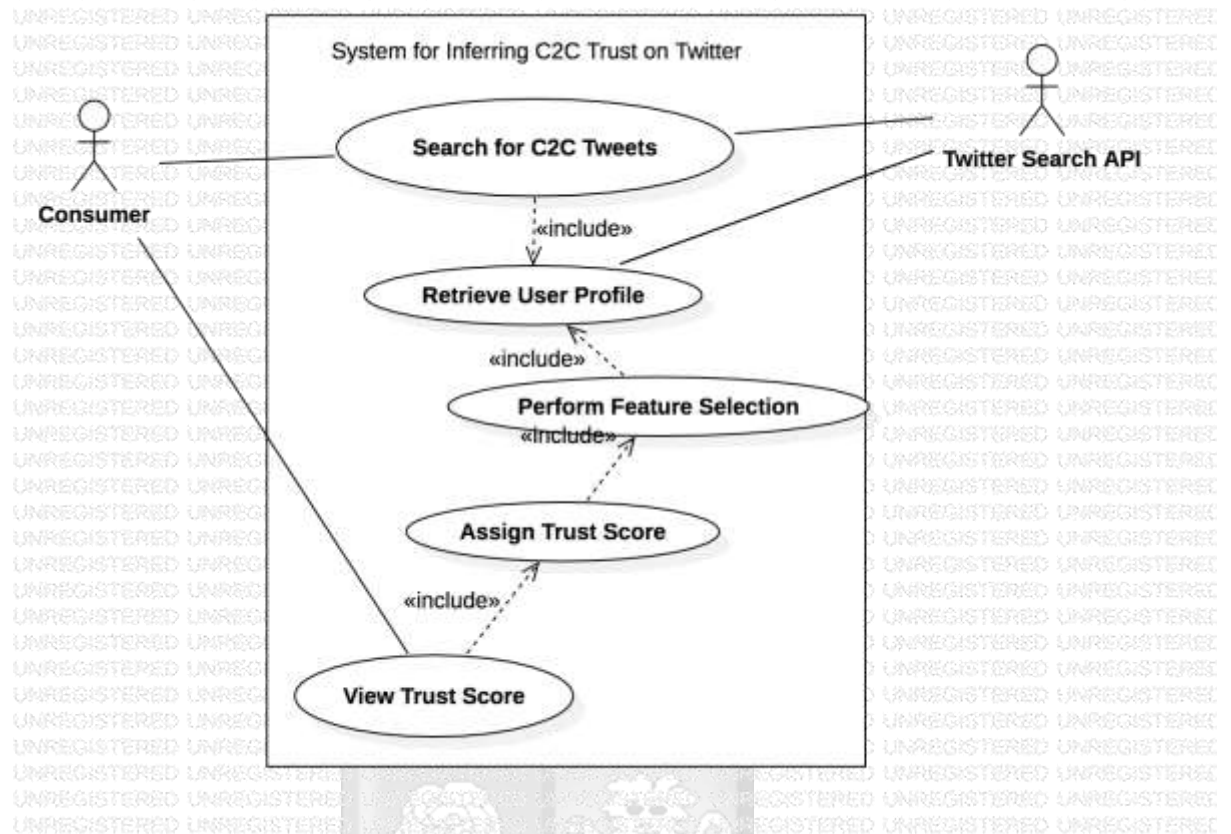


Figure 4.2 : Proposed Algorithm Use Case

4.5.2 Detailed Use Case Descriptions

This section provides comprehensive descriptions for the use cases in Figure 4.3 in a two- column fully dressed format.



<p>Use case: Search Tweets, Collect Tweets</p> <p>Primary Actors</p> <p>User</p> <p>Twitter Search API</p> <p>Preconditions</p> <p>Search Tweets use case completed successfully</p> <p>User has access to Twitter Search API</p> <p>Post conditions</p> <p>System collects tweets from Twitter Search API matching the keywords provided</p> <p>Main Success Scenarios</p>	
Actor Intention	System Responsibility
1. User enters the keywords to be used	<p>2. Pass keywords entered as parameter to be used to collect tweets</p> <p>3. Collect tweets from Twitter Search API using the keywords entered</p> <p>4. Save tweets collected</p> <p>5. Extract Twitter profile features</p>
6. View user profile loaded	

Figure 4.3 : Search Tweets Use Case

Use case: Assign Trust Score Primary Actors User Application Preconditions User profile data is retrieved and stored successfully Post conditions User is correctly assigned a trust score Main Success Scenarios	
Actor Intention	System Responsibility
1. User initiates context of trust assignment	2. System initiates feature selection 3. Selected features are loaded into system 4. Compute trust score based on selected features and judgement matrix 4. Return trust score 5. Save trust score of a user
6. View trust score of user	

Figure 4.4 : Assign Trust Score Use Case

4.5.3 Sequence Diagram

A flow chart diagram, it describes the sequence of operations the algorithm undertakes from start to completion. The sequence diagram is depicted in Figure 4.6.

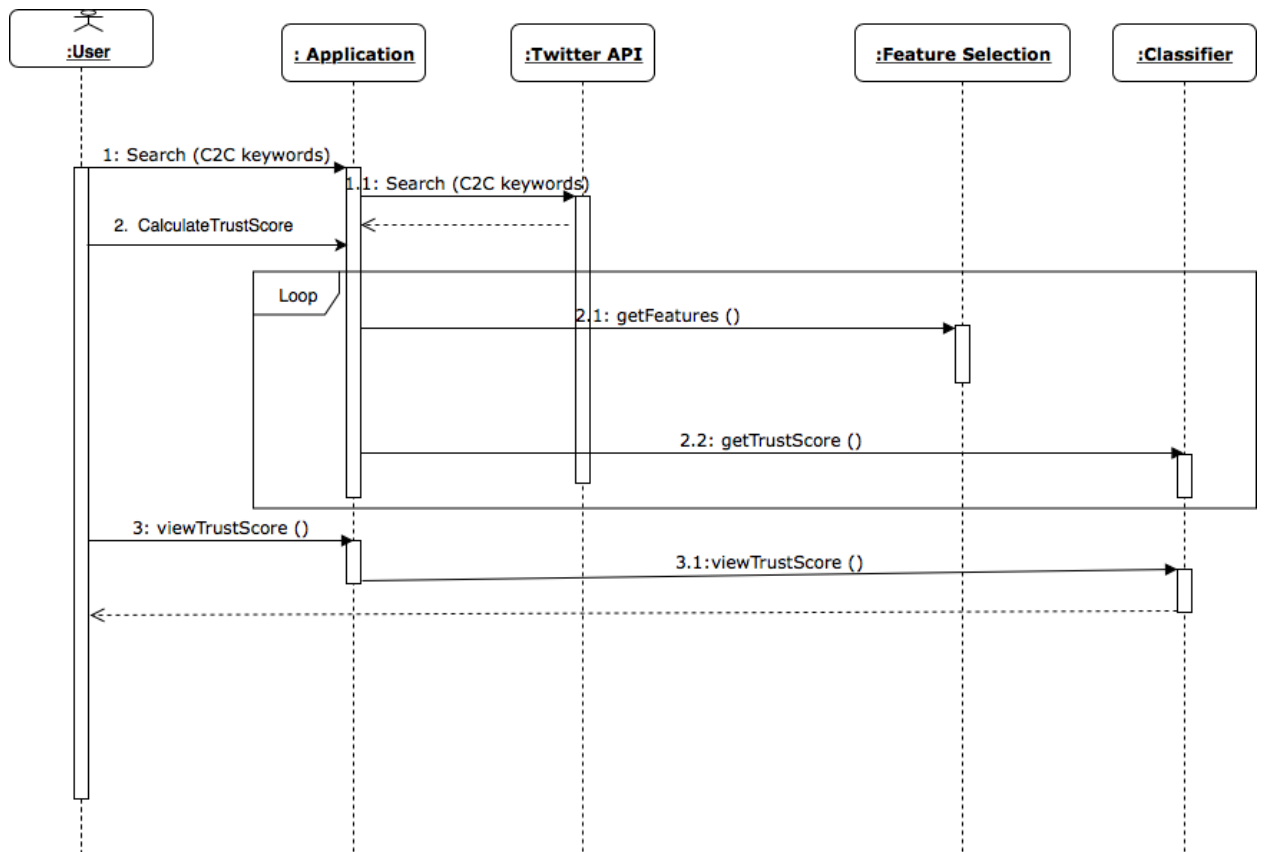


Figure 4.5 : Sequence Diagram

4.5.4 Context Diagram

Context diagram as shown in Figure 4.6 illustrates the boundary of the proposed model, its environment and entities that interact with it. Entities that interact with the proposed algorithm are a user and Twitter Search API. The user searches for C2C keywords to the Twitter Search API. The model gets features relevant to the trust context and assigns a trust score to consumer and communicates this information to the user.

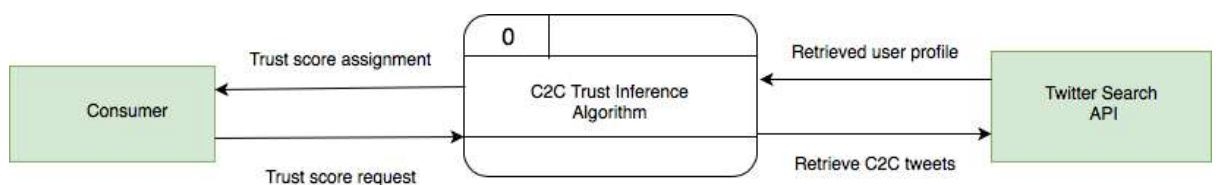


Figure 4.6: Context Diagram

4.5.5 Data Flow Diagram

A data flow diagram describes the movement of data through processes included in the algorithm. Figure 4.7 shows level 0 Data Flow Diagram (DFD).

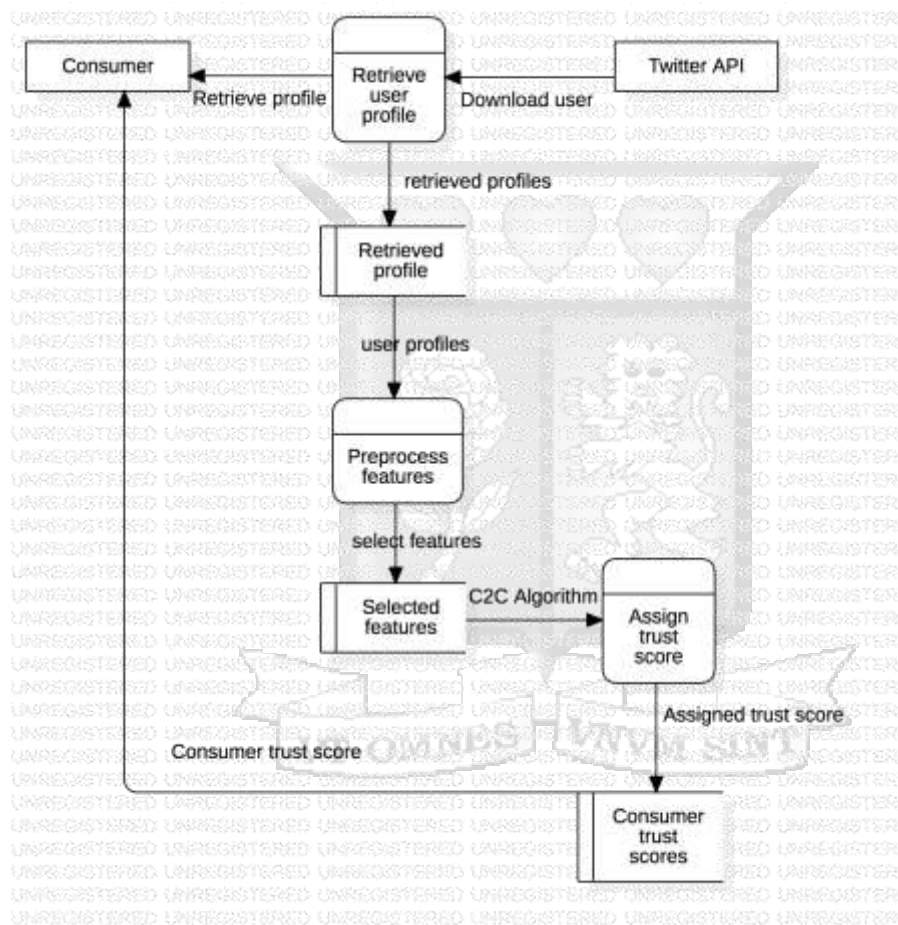


Figure 4.7 : Level 0 DFD

Chapter 5: Algorithm Implementation and Validation

5.1 Introduction

This chapter describes how the proposed algorithm was implemented, tested and validated. The process of building a corpus for machine learning is the first step in the process of implementing the algorithm. It is the researchers view that the proposed algorithm is applicable to other social media platforms as well. The algorithm was then tested with the selected features using KNN and RF machine learning algorithms for the single context and with the rest of the features under consideration.

5.2 Building the Dataset

The generation of corpus of tweets from sampled Twitter users who had engaged in consumer-to-consumer e-commerce was generated using R functions for Exploratory software. R functions for Exploratory package provides a set of utility functions to make data wrangling and analysis work better. To create the corpus of user profiles, the researcher considered only those keywords that are related to C2C e-commerce. The keyword used was the hashtag “#IkoKaziKE” translating to “there is work in Kenya” which had consumers selling and buying various services. User Twitter profiles were pre-processed by removing features that were not contributing to this research and therefore not considered by the model.

The dataset consisted of 30,102 tweets by 199 user unique users. We used domain experts who provided trust scores to estimate the trust score of a consumer in particular context. The dataset had users labelled with trust scores as follows: 47 users were assigned 5, 41 users were assigned 4, 45 users were assigned 3, 37 users were assigned 2 and finally 29 users were assigned 1. Consumers trust score of 4 and above (out of 5) was taken to be very trustworthy while a trust score of 2 or less was taken to be less trustworthy. A trust score of 3 was assumed to be neutral. The KNN and RF algorithms discussed in section 2.12 were used to solve the multi-class problem. The dataset is described in Figure 5.1.

```
Trust_score
1      29
2      37
3      45
4      41
5      47
dtype: int64
```

Figure 5.1: Dataset Description

The csv dataset was loaded to into Pandas DataFrame as detailed in Figure 5.2.

```
#importing the datasets and loading them in a data frame
data_store = "c2c2data.csv" #Assigning data set variable
raw_data = pd.read_csv (data_store) #reading the dataset with pandas
raw_data_new = raw_data.drop(['user_id', 'account_created_at'], axis = 1)
data_pandas = pd.DataFrame(raw_data_new)

#printing the dataset
print(data_pandas)
```

Figure 5.2 : Loading Data to Pandas DataFrame

The DataFrame is thereafter converted to Numpy-array representation as shown in Figure 5.3.

```
#Getting the values in the numpy array and grouping it
f1 = raw_data['retweet_count'].values
f2 = raw_data['followers_count'].values
f3 = raw_data['friends_count'].values
f4 = raw_data['subscribed_count'].values
f5 = raw_data['statuses_count'].values
f6 = raw_data['liked_tweets_count'].values
f7 = raw_data['Trust_score'].values
```

Figure 5.3 : Numpy-array Representation of Training Data

5.3 Training the Model

The researcher used scikit-learn for implementation (Pedregosa, Varoquaux, Gramfort, & Thirion, 2011). Scikit-learn is a python library that focuses on bringing machine learning to non-specialist using general-purpose high-level language. Sklearn RFE was used for feature selection with logistic regression. The classification algorithm used is not necessarily the preferred algorithm to be used in modelling the problem (Muchiri, Ateya, & Wanyembi, 2019). To train the model, the csv data file containing the preprocessed and labelled user profiles was

read into Pandas DataFrame. The corpus was split on 7:3 ratios for training and testing respectively using the train_test_split method of the scikit-learn library (Scikit-learn, 2019).

The algorithms used to train the model were KNN and RF. For KNN the researcher used Euclidean distance as parameter and for RF, entropy was preferred. The model was then tested for each of the proposed algorithms using the wrapper method by varying the number of selected features as input for each algorithm in an incremental manner.

5.4 Testing the Model

The test set (30 % of the labelled data) was used to validate the model. The test set was passed to the learnt model to be predicted and the results of the prediction compared with the actual labels. A confusion matrix without normalization to describe the performance of the algorithm is presented in Table 5.1 and Table 5.2 for KNN and RF classifiers respectively.

Table 5:1 : Confusion Matrix for KNN

		Predicted Trust Score				
		Class 1	Class 2	Class 3	Class 4	Class 5
Actual Trust Score	Class 1	8	0	0	0	0
	Class 2	3	4	5	1	1
	Class 3	0	2	5	4	2
	Class 4	0	2	3	5	4
	Class 5	0	0	1	4	6

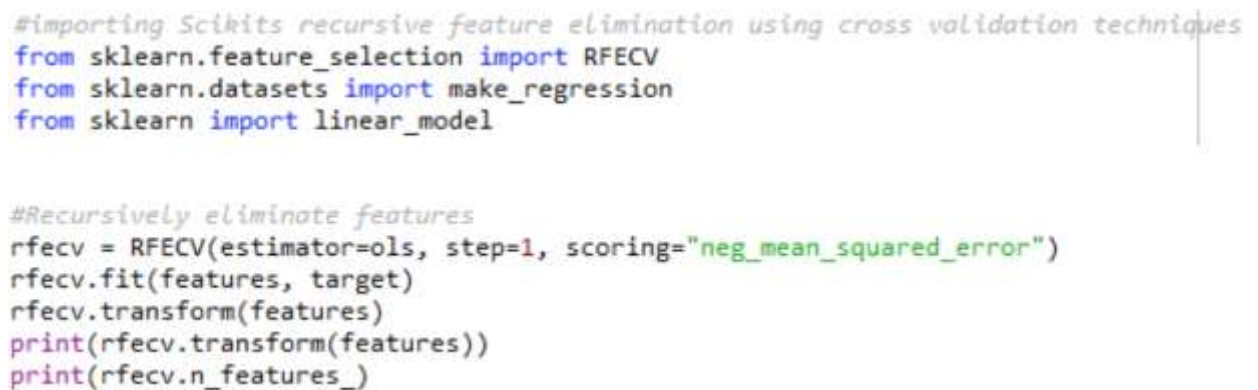
Table 5:2 : Confusion Matrix for RF

		Predicted Trust Score				
		Class 1	Class 2	Class 3	Class 4	Class 5
Actual Trust Score	Class 1	4	1	1	0	0
	Class 2	4	3	3	0	2
	Class 3	1	0	5	0	1
	Class 4	0	3	6	6	4
	Class 5	0	0	3	1	12

Figure 5.1 and Figure 5.2 can be interpreted as per the explanation in section 3.10. The confusion matrix was constructed where diagonal entries running from the top left to bottom right represent correctly classified samples and the rest represent misclassifications.

5.5 Using the Model for Feature Selection

Recursive Feature Elimination (RFE) method was used for feature selection. It works by recursively removing attributes and building a model on those attributes that remain. It uses the model accuracy to identify which attributes (and combination of attributes) contribute the most to predicting the target attribute (Bakharia, 2016). Logistic Regression was used to create a base classifier to evaluate a subset of attributes. Figure 5.4 shows the implementation of RFE with Logistic Regression.



```
#importing Scikits recursive feature elimination using cross validation techniques
from sklearn.feature_selection import RFECV
from sklearn.datasets import make_regression
from sklearn import linear_model

#Recursively eliminate features
rfecv = RFECV(estimator=ols, step=1, scoring="neg_mean_squared_error")
rfecv.fit(features, target)
rfecv.transform(features)
print(rfecv.transform(features))
print(rfecv.n_features_)
```

Figure 5.4 : Feature Selection with Logistic Regression Module

The RFE model was created and the model selected 2 attributes. RFE module selected the top two features as follower_count and subscribed count as per Figure 5.5.

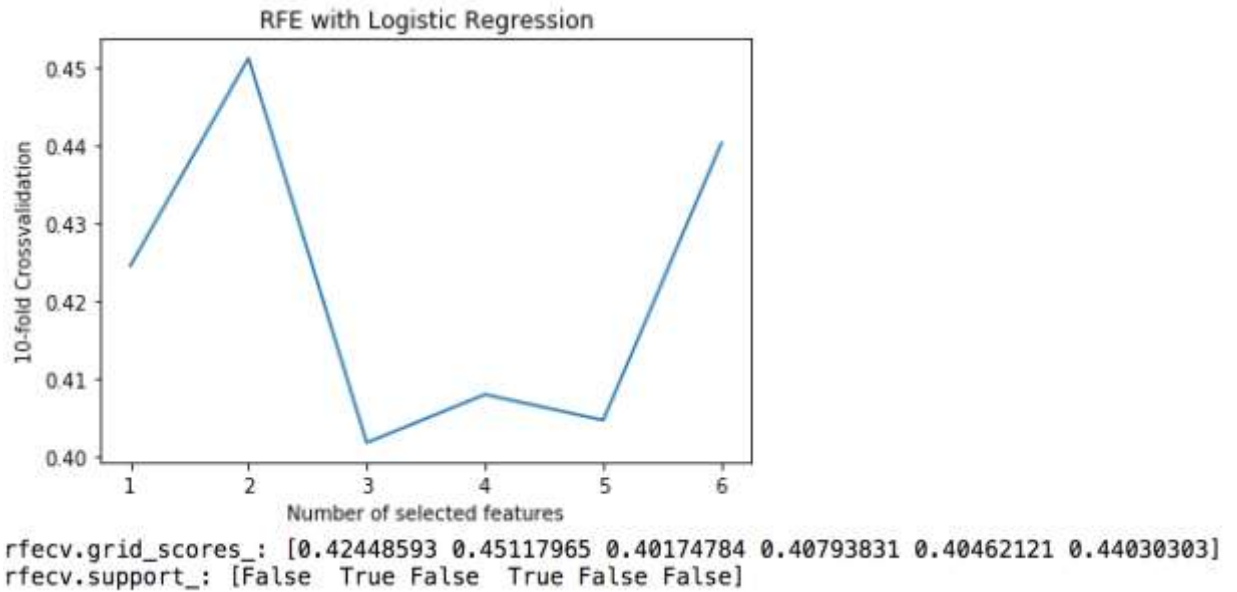


Figure 5.5 : Feature Selection using Logistic Regression

5.6 Validation

Validation of the algorithm was done in order to ascertain that the algorithm was able to infer a trust score for a Twitter user engaged in consumer-to-consumer e-commerce. The algorithm was validated to meet one of the research objectives of this study.

5.7 Trust Score Assignment with All Features

In this section, we look at the relationship between the all features and trust score from the dataset. The features in the dataset were user_id, retweet_count, followers_count, friends_count, listed_count, statuses_count, favourites_count and created_at to predict the trust score. User_id and created_at were not used in trust score assignment because they were not of importance to trust score prediction. This is evidenced from the in the seceding figure. Figure 5.6 shows the feature comparison in the dataset.

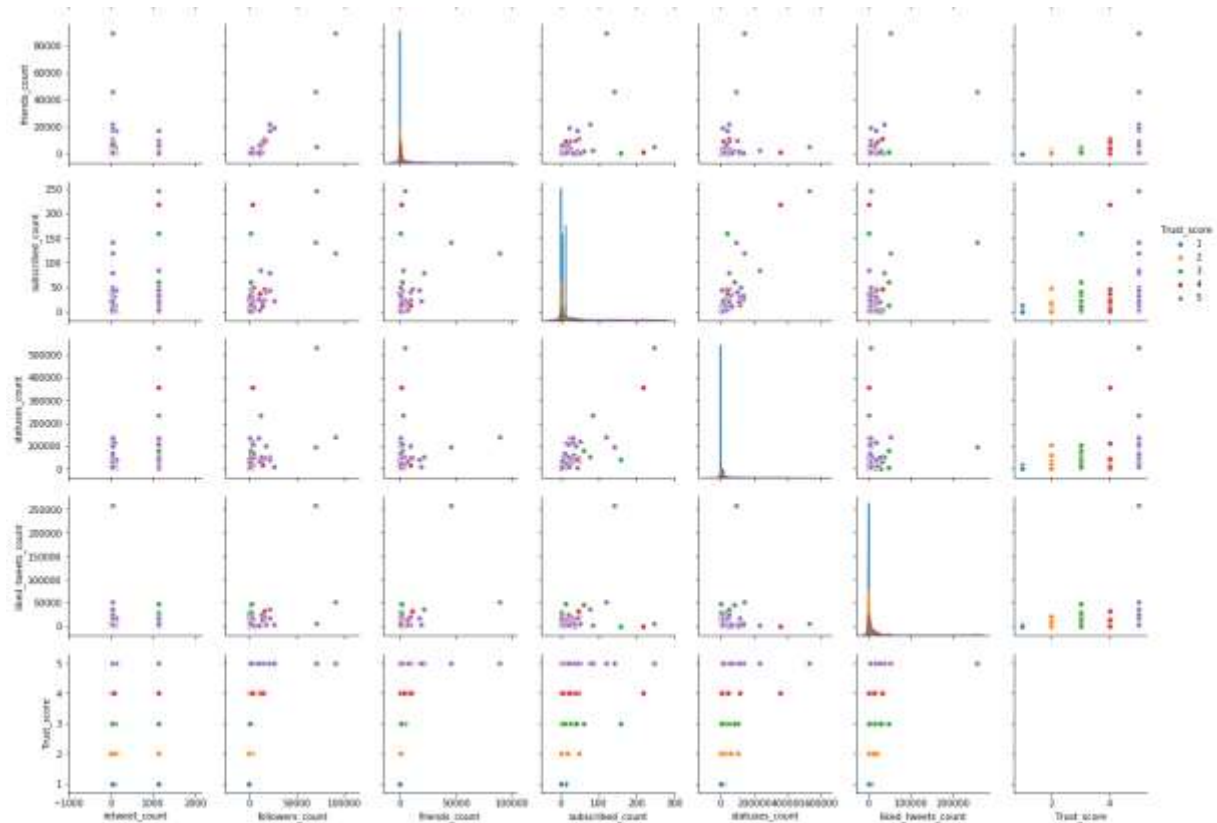


Figure 5.6 : Feature Comparison

5.8 Trust Score with Selected Features

After performing features selection using the wrapper techniques implemented using RFE, follower_count, and listed_count were found to be of importance in the prediction of the trust score. Our model therefore considered only these 2 features in its final prediction of the trust score. The accuracy of our algorithm using KNN was 0.58.

Chapter 6: Discussions

6.1 Introduction

This chapter discusses the results of the research in light of the objectives set out at the beginning of this research. The objectives of this research were to investigate factors that are important for establishing trust in C2C e-commerce on social media, review of existing models and algorithms used in C2C e-commerce sites to determine context-aware trust among consumers, the development of a context-aware algorithm for consumer-to-consumer trust on social media. The other objective was to validate the proposed algorithm. Twitter as a social media platform was used, where consumers were assigned a trust score based on selected features from their profiles.

This was done with a view of understanding the challenges faced by both social media users and providers due to lack of trust on social media specifically consumers who want to engage in consumer-to-consumer e-commerce. The adoption of the proposed algorithm by social will help in curbing C2C fraud on social media and improve trust among users thereby reducing uncertainty amongst buyers and sellers on social media platforms.

6.2 Discussions

In this research we developed an algorithm for inferring consumer-to-consumer trust on social media. We used Twitter as a case study but our research is applicable to other social media networks. The issue of trust on social media has majorly been around information credibility and detection of fraudulent/fake accounts, we therefore investigated an area that is fast gaining popularity among social media user, consumer-to-consumer e-commerce and which has a potential positive application on social media providers. This area has hitherto to be researched according to reviewed literature. We collected Twitter profiles of users who have engaged in C2C e-commerce on social media. We then selected features that can be of most use to in the development of this algorithm.

The algorithm assigns a user a trust score based on the selected features and the weights assigned to these features for a specific context. The trust scores are in the range of 1 to 5. 1 and 2 being less trustworthy consumers, we consider 3 as neutral and 4 and 5 as being of high trustworthiness for specific context. Using classification techniques to measure its accuracy in

terms of correctly assigning a user a trust score further validates the algorithm. Various supervised machine learning algorithms were used. We demonstrated that using this algorithm we were able to assign a consumer a trust score based on selected features for a specific context. We further, demonstrated that we were able to correct classify a consumer with an accuracy of 0.58.

6.3 Limitations of the Proposed Algorithm

The limitation imposed by social media provider's limits the amount of data that can be pulled by the API's. Further, algorithm is largely dependent on a judgement matrix for a specific context, which might limit its accuracy if not properly constructed.



Chapter 7: Conclusion and Recommendations

7.1 Conclusion

The section outlines step by step how the objectives of this research study were met. The first objective spelt out in this research was to investigate factors that are important for establishing trust in C2C e-commerce on social media. This study reveals are several factors that are crucial in establishing trust in C2C e-commerce. First, users need to trust the platform they use for engaging in C2C e-commerce as detailed in section 2.3 of this research. Secondly, users have to trust each other to certain degree to engage with a consumer or user they have or may never interact with in the physical world. They therefore turn to the social media community to for trust information. Social media community represents it contribution through features such as number of followers, number of friends among others.

The second objective was review existing models and algorithms used in C2C e-commerce to determine context-aware trust among consumers on social media. This was done with a view of understanding existing context-aware algorithms and models for inferring C2C trust on social media. The researcher reviewed, compared and contrasted literature on the existing models and algorithms, to identify gaps were addressed by the proposed algorithm. Those include application of multi-class classification and wrapper feature selection technique. This research took an interaction-based approach to computing the trust score of a social media user engaged in C2C e-commerce.

The third objective was to develop a context-aware algorithm for C2C trust on social media. The conceptual model presented in section 2.13 showed an overview of the framework to infer the trust score of a social media user engaged in C2C e-commerce. The develop algorithm was discussed in detail under section 4.2 of analysis and design. The algorithm incorporated an offline judgment matrix, λ , for assigning weights to the selected features. The algorithm considered features that change infrequently or those that change gradually. The results of the testing and training of the algorithm are discussed in detail under section 5.4 and 5.5.

Finally, the algorithm was validated as per the results shown in section 5.6. The algorithm was validated using all the features and using only those features selected through the wrapper technique. The results from the experiment with only selected features were encouraging.

7.2 Recommendations

This research showed that a consumer's trust score could be inferred using social media features. Twitter was used a case study, to generate the trust score, feature selection was performed by the algorithm for each consumer profile from the initial nine features. Weights obtained from supervised machine learning models were then applied to these features to generate the final trust score for a consumer. The trust score presented by our algorithm is only a partial representation of a user social media activity.

7.3 Future Work

In as much as our research concludes at this point, in the near future, the algorithm should be able to aggregate metadata from more social media platforms. As such, the proposed algorithm should be able handle the increased number of features from the different social media platforms with better accuracy. This will enable the algorithm to scale and adopted across various platforms. Also, we plan on incorporating sentiment analysis to capture consumer feedback for the various sellers and buyers on social media using textual data. This research appreciates that social media only represents a fraction of a consumers online transactions activities therefore recommends that data such as mobile money transactions could be incorporated in future works through the use of a mobile application.



References

- Abdul-Rahman, A., & Hailes, S. (2000). Supporting Trust in Virtual Communities. *HICSS* .
- Šitum, M. (2014). *Analysis of Algorithms For Determining Trust Among Friends on Social Networks*. Master Thesis, University of Zagreb, Faculty of Electrical Engineering and Computing, Vienna.
- Artz, D., & Gil, Y. (2007). A survey of trust in computer science and the semantic web. *Journal of web semantics: science, services and agents on the World Wide Web*.
- Baghdadi, Y. (2013). From E-commerce to Social Commerce: A Framework to Guide Enabling Cloud Computing. *Journal of theoretical and applied electronic commerce research* , 8 (3).
- Bao, N., & Volkovynska, A. (2016). *Factors that stimulate sellers to engage in C2C commercial activity on social networking platforms*. Lund University, Department of Informatics.
- Boyd, D. M., & Ellison, N. B. (2007). Social Network Sites: Definition, History, and Scholarship. *Journal of Computer-Mediated Communication* , 13 (1), 210–230.
- Bryman, A., & Bell, E. (2011). *Business Research Methods* (3rd edition ed.). New york, USA: Oxford University Press.
- Chahal, M. (2016, March). *Social commerce: How willing are consumers to buy through social media?* Retrieved January 2019 from MarketingWeek: <https://www.marketingweek.com/2016/03/23/social-commerce-how-willing-are-consumers-to-buy-through-social-media/>
- Chen, J. V., Su, B.-c., & Widjaja, A. E. (2016). Facebook C2C social commerce: A study of online impulse buying. *Decision Support Systems Volume* , 83, 57-69.
- Communications Authority of Kenya. (2018). *Annual Report*. From Communications Authority of Kenya: <https://ca.go.ke/wp-content/uploads/2018/04/Annual-Report-for-the-Financial-Year-2016-2017.pdf>
- Creswell, J. W. (2009). *Research Design* (3rd Edition ed.). Los Angeles: SAGE.
- Dan, C. (2014). Consumer-to-consumer (C2C) electronic commerce: the recent picture . *International Journal of Networks and Communications* , 4 (2), 29-32 .
- Digital Commerce 360. (2018, February). *Internet Retailer*. From Digital Commerce 360: <https://www.digitalcommerce360.com/article/us-ecommerce-sales/>

- Dignan, L. (2019, February). *Fixing Facebook: Why it Needs a Trust Score*. From Zdnet: https://www.zdnet.com/google-amp/article/fixing-facebook-why-it-needs-a-trust-score/?__twitter_impression=true
- Facebook. (2018, January). *Graph API*. From Facebook: <https://developers.facebook.com/docs/graph-api/>
- Fisher, R. A. (2007). *Statistical Methods for Research Workers*. Edinburgh, England: Kalpaz Publications.
- Gefen, D., & Straub, D. (2003). Managing User Trust in B2C e-Services. *E-Service Journal*, , 2 (2), 7-24.
- Golbeck, J., & Hendler, J. (2005). *Inferring Trust Relationships in Web-based Social Networks*. Maryland.
- Gustavsson, M., & Johansson, A.-M. (2006). Consumer Trust in E-commerce.
- Han, J., Kamber, M., & Pei, J. (2012). *Data Mining: Concepts and Techniques* (3rd Edition ed.). Boston: Elsevier Inc.
- Heijden, H. v., Verhagen, T., & Creemers, M. (2003). Understanding online purchase intentions: contributions from technology and trust perspectives. *European Journal of Information Systems*, 2003 (12), 41-48.
- Jones, K., & Leonard, L. N. (2007). Consumer-to-Consumer Electronic Commerce: A Distinct Research Stream. *Journal of Electronic Commerce in Organizations*, 5 (4), 39-54.
- Kinater, M., & Rothermel, K. (2003). *Architecture and Algorithms for a Distributed Reputation System*. Berlin, Germany: Springer-Verlag.
- Kumah, M. K. (2014). The Role of Social Media as a Platform for E-Commerce.
- Lackey, K., & Graham, J. (2019, January). *Technology*. Retrieved February 2019 from USA Today: <https://www.usatoday.com/story/tech/news/2019/01/21/facebook-owned-whatsapp-limits-number-forwards-combat-fake-news/2636179002/>
- Laudon, K. C., & Traver, C. G. (2014). *E-Commerce 2014* (Tenth ed.). Pearson Education.
- Lee, M. K., & Turban, E. (2001). A Trust Model for Consumer Internet Shopping. *International Journal of Electronic Commerce*, 6 (1), 75-91.
- Malthouse, E., Haenlein, M., Skiera, B., Wege, E., & Zhang, M. (2013). Managing Customer Relationships in the Social Media Era: Introducing the Social CRM House. *Journal of Interactive Marketing*, 27, 270–280.
- Martin, E. (2017). *The Evolving Role of Social Media in Ecommerce*. From Entrepreneur: <https://www.entrepreneur.com/article/288952>

- Menzies, F. (2016, April). *Why Consumer-to-Consumer Communication Wins*. (Forbes) Retrieved January 2019 from Forbes: <https://www.forbes.com/sites/gyro/2012/04/26/why-consumer-to-consumer-communication-wins/#5484a9794b17>
- Merriam-webster. (2018). *Definition of trust*. From Merriam-webster: <https://www.merriam-webster.com/dictionary/trust>
- Mui, L., Mohtashemi, M., & Halberstadt, A. (2002). A computational model of trust and reputation. *Proceedings of the 35th Hawaii International Conference on System Sciences* . ResearchGate.
- Naz, R., & Khan, M. N. (2015). Rapid Applications Development Techniques: A Critical Review. *International Journal of Software Engineering and Its Applications* , 9 (11), 163-176.
- Resnick, P., & Zeckhauser, R. (2002). Trust among Strangers in Internet Transactions: Empirical Analysis of eBay's Reputation System. *The Economics of the Internet and E-commerce* , 11, 127 - 157.
- Richard, J. E., & Guppy, S. (2014). Facebook: Investigating the influence on consumer purchase intention. *Asian Journal of Business Research* , 4 (2), 1-15.
- Russell, M. A. (2013). *Mining the Social Web* (2nd ed.). O'Reilly Media Inc.
- Sarantakos, S. (2013). *Social Research* (4th ed.). London: Palgrave Macmillan .
- Saunders, M., Lewis, P., & Thornhill, A. (2009). *Research methods for business students* (5th Edition ed.). Harlow, England: Pearson Education.
- Sherchan, W., Nepal, S., & Paris, C. (2013). A Survey of Trust in Social Networks. *Association of Computing Machinery (ACM)* , 45 (4), 33.
- Staab, E., & Engel, T. (2008). *Combining Cognitive and Computational Concepts for Experience-Based Trust Reasoning*. University of Luxembourg. Luxembourg: Association for the Advancement of Artificial Intelligence.
- Stephen, A. T., & Toubia, O. (2009). Deriving Value from Social Commerce Networks. *Journal of Marketing Research*.
- Svec, T., & Samek, J. (2017). *Trust Evaluation on Facebook using Multiple Contexts*. Brno University of Technology, Faculty of Information Technology.
- Taherian, M., Amini, M., & Jalili, R. (2008). Trust Inference in Web-Based Social Networks using Resistive Networks. *The Third International Conference on Internet and Web Applications and Services* .

- Thaw, Y. Y., & Mahmood, A. K. (2009). A Study on the Factors That Influence the Consumers' Trust on E-commerce Adoption . (*IJCSIS*) *International Journal of Computer Science and Information Security* , 4 (1&2), 153-159.
- Transparency Market Research. (2017). *C2C E-commerce Market - Global Industry Analysis, Size, Share, Growth, Trends and Forecast 2016 - 2024*. From Transparency Market Research: <https://www.transparencymarketresearch.com/c2c-ecommerce-market.html>
- Twitter. (2019, February). *Developer*. (Twitter, Producer) From Twitter: <https://developer.twitter.com/en/docs>
- Wang, Y., & Vassileva, J. (2007). Toward Trust and Reputation Based Web Service Selection: A Survey. *Int'l Trans. Systems Science and Applications* , 3, 118-132.
- Wickham, H., & RStudio. (2018, December). *httr: Tools for Working with URLs and HTTP*. Retrieved 2019 from CRAN.R-PROJECT : <https://cran.r-project.org/web/packages/httr/index.html>
- Ye, B. (2018). *Trust Management in Crowdsourcing Environments*. Macquarie University , Department of Computing. Sydney: Macquarie University .
- Yu, S., & Guo, S. (2016). *Big Data Concepts, Theories and Applicalications*. New York: Springer.
- Zhang. (2014). *Context-Aware Transaction Trust Computation in E-Commerce Environments*. Macquarie University, Department of Computing. Sydney: Macquarie University.
- Zhang, H., Chen, D., & Sun, R. (2010). The study of consumer trust in C2C e-commerce based on reputation score, information disclosure Online Consumer Review quality. *International Conference on Management of e-Commerce and e-Government* , 184-187.
- Ziegler, C.-N., & Lausen, G. (2005). Propagation Models for Trust and Distrust in Social Networks. *Information Systems Frontiers* , 4 (5), 337-358.

Appendix A: Originality Report

feedback studio

A Context-Aware Algorithm for Consumer-to-Consumer Trust on Social Media

By
Dennis Loyatum
101084

Match Overview

22%

1	Submitted to Graduate...	2%
2	Submitted to London S...	1%
3	iprvi.org	1%
4	Submitted to Adelaide ...	1%
5	pdfs.semanticscholar...	1%
6	Vespa Simkovic, Vedra...	1%
7	editionsnyc.com	1%
8	www.businessnewsch...	1%
9	Submitted to Higher Ed...	<1%
10	socialnetworks.org	<1%
11	Hansheng Zhang, Dong...	<1%

